

IBM

eserver

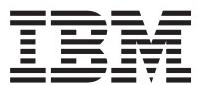
iSeries

iSeries Access for Web

Version 5

SC41-5518-01





eserver

iSeries

iSeries Access for Web

Version 5

SC41-5518-01

Note

Before using this information and the product it supports, be sure to read the information in Appendix G, "Notices" on page 131.

Second Edition (August 2002)

This edition replaces SC41-5518-00. This edition applies only to reduced instruction set computer (RISC) systems.

© Copyright International Business Machines Corporation 1999, 2002. All rights reserved.

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

About iSeries Access for Web (SC41-5518-01)	v	
Who should read this book	v	
Conventions and terminology used in this book	v	
Prerequisites and related information	v	
How to send your comments	vi	
Part 1. Getting Started	1	
Chapter 1. Before You Start	3	
What is iSeries Access for Web?	3	
What is IBM WebSphere Host Publisher?	3	
What's New for V5R2	3	
License Information	5	
Chapter 2. iSeries Access for Web Setup Checklist	7	
iSeries Setup Considerations	8	
WebSphere Setup Considerations	8	
Part 2. iSeries Setup and Installation	9	
Chapter 3. Install iSeries Access for Web on the iSeries server	11	
iSeries Server Hardware Requirements	11	
iSeries Server Software Requirements	12	
Web Browser Requirements	14	
Beta Release	15	
Install iSeries Access for Web	16	
Install PTFs	16	
Preparation for creating the HTTP Server	18	
HTTP setup for WebSphere 4.0	19	
WebSphere 4.0 Advanced Edition Environment	22	
WebSphere 4.0 Advanced Single Server Edition	22	
ASF Tomcat Server	23	
Upgrade iSeries Access for Web to V5R2	25	
Configure iSeries Access for Web	25	
Install IBM Host Publisher 4.0	27	
Verify the Installation	29	
Performance Tuning	30	
Delete iSeries Access for Web and Host Publisher	31	
Chapter 4. Security	33	
General	33	
Secure HTTP (HTTPS)	33	
Part 3. Using iSeries Access for Web	39	
Chapter 5. Using iSeries Access for Web	41	
Introduction	41	
Print	42	
Messages	46	
5250	49	
Database	49	
Files	58	
Jobs	61	
Command	62	
Mail	64	
My Folder	65	
Customize	65	
Other	66	
Chapter 6. Restrictions	69	
Print	69	
Messages	69	
Database	69	
Files	72	
Command	72	
Web Browsers	72	
Part 4. Administering and Customizing iSeries Access for Web	73	
Chapter 7. iSeries Access for Web Policies	75	
Introduction	75	
General	75	
Print	78	
Messages	81	
Jobs	82	
5250	84	
Database	85	
Files	88	
Command	91	
Mail	92	
My Folder	93	
Administration	94	
Other	96	
Chapter 8. Preferences	99	
Introduction	99	
Categories of Preferences	99	
Use Preferences	99	
Restrict Access to Preferences	100	
Chapter 9. Administering Users and Groups	101	
Introduction	101	
Determine Policy Settings for a User	101	
Customize User Profiles	102	
Customize Group Profiles	103	
Strategies for Customizing iSeries Access for Web	104	

Chapter 10. Customize the Home Page and Template File	105
<hr/>	
Part 5. Appendixes	107
Appendix A. Sources of Information for iSeries Access for Web	109
Information Authorized Program Analysis Report (Information APAR) and PTF	109
iSeries Access for Web Information on the Web . .	110
iSeries Access for Web Read Me File.	110
Appendix B. Save and Restore	111
iSeries Access for Web	111
Appendix C. NLS Considerations	113
Language and Character Set Selection	113
Information in Multiple Languages (Multilingual) .	113
CCSIDs and OS/400 Messages	114
Appendix D. Enrolling Users if You Use Document Library Services File System (QDLS).	115
Appendix E. CL Commands used with iSeries Access for Web	117
CFGACCWEB2 (Configure iSeries Access for Web)	
Command	117
STRACCWEB2 (Start iSeries Access for Web)	
Command	121
ENDACCWEB2 (End iSeries Access for Web)	
Command	123
RMVACCWEB2 (Remove iSeries Access for Web)	
Command	125
Appendix F. Problems and Problem Reporting	129
Technical Support	129
Problem Reporting—Gathering Information for IBM Support	129
Appendix G. Notices	131
Code disclaimer information	132
Trademarks	133
Index	135

About iSeries Access for Web (SC41-5518-01)

This book contains directions for installing iSeriesTM Access for Web and WebSphere[®] Host Publisher on the iSeries server. A checklist is provided to guide you through the steps you need to complete to use iSeries Access for Web. Familiarity with the iSeries server is strongly recommended.

Installation and configuration is necessary only on the iSeries server. This book assumes that the system administrator will install and configure the iSeries server.

This product includes software developed by the Apache Software Foundation (<http://www.apache.org/>).

Who should read this book

You should read this book if you want to learn more about how to use iSeries Access for Web, or if you are responsible for installing and configuring iSeries Access for Web and WebSphere Host Publisher.

Conventions and terminology used in this book

Several conventions are used throughout this book:

- **WebSphere AE** is used throughout this book to represent IBM[®] WebSphere Application Server Advanced Edition version 4.0.2.
- **WebSphere AEs** is used throughout this book to represent IBM WebSphere Application Server Advanced Single Server Edition version 4.0.2.
- **Tomcat** is used throughout this book to represent Apache Software Foundation Tomcat version 3.2.4.
- **ASF** is used to represent Apache Software Foundation.
- **Host Publisher** is used throughout this book to represent IBM WebSphere Host Publisher version 4.0.
- **Web server** is used throughout this book to represent IBM HTTP Server for iSeries.
- **Web application server** is used throughout this book to represent WebSphere AE, Websphere AEs, and Tomcat.
- **Server name** is used throughout this book to represent the name of your iSeries server.
- **V5Rx** is used throughout this book to represent Operating System/400[®] Version 5 Release 1 or Release 2.

Prerequisites and related information

Use the iSeries Information Center as your starting point for looking up iSeries technical information.

You can access the Information Center two ways:

- From the following Web site:
<http://www.ibm.com/eserver/iseries/infocenter>
- From CD-ROMs that ship with your Operating System/400 order:
iSeries Information Center, SK3T-4091-02. This package also includes the PDF versions of iSeries manuals, *iSeries Information Center: Supplemental Manuals*, SK3T-4092-01, which replaces the Softcopy Library CD-ROM.

The iSeries Information Center contains advisors and important topics such as Java™, TCP/IP, Web serving, secured networks, logical partitions, clustering, CL commands, and system application programming interfaces (APIs). It also includes links to related IBM Redbooks™ and Internet links to other IBM Web sites such as the IBM home page.

With every new hardware order, you receive the *iSeries Setup and Operations* CD-ROM, SK3T-4098-01. This CD-ROM contains IBM @server iSeries Access for Windows and the EZ-Setup wizard. iSeries Access offers a powerful set of client and server capabilities for connecting PCs to iSeries servers. The EZ-Setup wizard automates many of the iSeries setup tasks.

For more information about iSeries Access, see the following:

- <http://www.ibm.com/eserver/iseries/access/>

iSeries Access for Web is part of the iSeries Access family. Use the iSeries Access Web site as a general source of information for the iSeries Access Family of products.

- Appendix A, Sources of Information for iSeries Access for Web

This is a list of additional sources of iSeries Access for Web information.

iSeries Navigator

IBM iSeries Navigator is a powerful graphical interface for managing your iSeries servers. iSeries Navigator functionality includes system navigation, configuration, planning capabilities, and online help to guide you through your tasks. iSeries Navigator makes operation and administration of the server easier and more productive and is the only user interface to the new, advanced features of the OS/400 operating system. It also includes Management Central for managing multiple servers from a central system.

You can find more information on iSeries Navigator in the iSeries Information Center and at the following Web site:

<http://www.ibm.com/eserver/iseries/navigator/>

How to send your comments

Your feedback is important in helping to provide the most accurate and high-quality information. If you have any comments about this book or any other iSeries documentation, fill out the readers' comment form at the back of this book.

- If you prefer to send comments by mail, use the readers' comment form with the address that is printed on the back. If you are mailing a readers' comment form from a country other than the United States, you can give the form to the local IBM branch office or IBM representative for postage-paid mailing.
- If you prefer to send comments by FAX, use either of the following numbers:
 - United States, Canada, and Puerto Rico: 1-800-937-3430
 - Other countries: 1-507-253-5192
- If you prefer to send comments electronically, use one of these e-mail addresses:
 - Comments on books:
RCHCLERK@us.ibm.com
 - Comments on the iSeries Information Center:
RCHINFOC@us.ibm.com

Be sure to include the following:

- The name of the book or iSeries Information Center topic.
- The publication number of a book.
- The page number or topic of a book to which your comment applies.

Part 1. Getting Started

Chapter 1. Before You Start	3
What is iSeries Access for Web?	3
What is IBM WebSphere Host Publisher?	3
What's New for V5R2	3
License Information	5

Chapter 2. iSeries Access for Web Setup

Checklist	7
iSeries Setup Considerations	8
WebSphere Setup Considerations	8

Chapter 1. Before You Start

This chapter contains critical information for iSeries system administrators and anyone else involved in using iSeries Access for Web.

What is iSeries Access for Web?

iSeries Access for Web (5722-XH2) is the latest offering in the iSeries Access (5722-XW1) family of products. It offers web browser based access to iSeries servers. iSeries Access for Web enables end users to leverage business information, applications, and resources across an enterprise by extending the iSeries resources to the client desktop through a web browser.

iSeries Access for Web has the following advantages:

- It is server based.
- It is implemented using Java Servlet technology.
- It uses industry standard protocols—HTTP, HTTPS, and HTML.
- It is lightweight, requiring only a browser on the client.
- It provides access to 5250 user interface, database, integrated file system, print, jobs, batch commands, and messages.

Host Publisher and Host Publisher Studio have been bundled with the 5722-XH2 iSeries Access for Web product to provide a complete web-to-host integration solution.

What is IBM WebSphere Host Publisher?

IBM WebSphere Host Publisher 4.0 (5724-B81) enables users to modernize host applications, or replace traditional character-based interfaces with a Web look and feel. These host applications can then be run directly from any standard Web browser. Host Publisher allows you to integrate multiple sources of data, including host and database applications, into a single Web page with no change to the backend applications.

Host Publisher and Host Publisher Studio have been bundled with the 5722-XH2 iSeries Access for Web product to provide a complete web-to-host integration solution.

For more information about Host Publisher, go to:
<http://www.ibm.com/eserver/iseries/access/hostpublisher/>

What's New for V5R2

New product identifier

V5R1 iSeries Access for Web was delivered with a product identifier of 5722-XH1 and supported WebSphere 3.5. In V5R2, a number of changes were made to iSeries Access for Web to make use of the technology available when running under WebSphere 4.0 or Apache Software Foundation Tomcat web application servers. These changes do not allow V5R2 iSeries Access for Web to support WebSphere 3.5.

To continue to support WebSphere 3.5 with V5R1 iSeries Access for Web, V5R2 iSeries Access for Web had to:

- Be built with a new, unique product identifier (5722-XH2)
- Install to a new, unique library (QIWA2)
- Install to a new, unique path in the integrated file system
 - /QIBM/ProdData/Access/Web2
 - /QIBM/UserData/Access/Web2
- Create new, unique, CL commands
 - Configure iSeries Access for Web (CFGACCWEB2)
 - Start iSeries Access for Web (STRACCWEB2)
 - End iSeries Access for Web (ENDACCWEB2)
 - Remove iSeries Access for Web (RMVACCWEB2)

Web Application Server support

V5R2 iSeries Access for Web supports the following web application servers on V5Rx iSeries servers:

- WebSphere 4.0 Advanced Edition
- WebSphere 4.0 Advanced Single Server Edition
- ASF Tomcat 3.2.4

WebSphere 3.5 users should continue to use V5R1 iSeries Access for Web.

Multiple administrative server support on WebSphere

Within the WebSphere environment, web applications are deployed and configured to run within a WebSphere administrative server. Multiple administrative servers can be configured to run concurrently within WebSphere.

V5R2 iSeries Access for Web can be configured to run within multiple WebSphere administrative servers concurrently. This support also allows you to configure iSeries Access for Web to run within multiple editions of WebSphere concurrently.

Multiple ASF Tomcat server support

Multiple ASF Tomcat servers can be configured and run concurrently. V5R2 iSeries Access for Web can be configured to run multiple ASF Tomcat servers concurrently just as it can for WebSphere.

PDF support

View, mail, or send printer output or Run SQL output in PDF format. The most advanced support makes use of IBM's Infoprint® Server (5722-IP1) licensed program product.

XML support

Copy data to table supports XML documents as an input file type.

File actions

Copy, rename, delete, and mail files in Browse files and Browse NetServer file shares function. Create, rename, and delete directories.

Jobs List and manage your jobs on the iSeries server. List and manage server jobs on the iSeries server that are running on your behalf. View job logs for active jobs or server jobs. View printer output for completed jobs.

Search commands

Search for specific CL commands to run by either providing partial command names or providing words contained in command text descriptions. Commands matching the search criteria are returned in a list.

My commands

Save previously run commands across browser sessions using the Save action of the Previous command list. Access saved commands through the My commands item.

Mail as attachment

Send the following types of information as an e-mail attachment, to anyone with an e-mail address:

- SQL output generated by Run SQL
- PDF output created from Printer output
- Integrated file system files using the Mail file action
- Command completion status generated by Run Command (can only be sent to the user's own e-mail address)

My Folder

Send items to your personal folder, accessible from the My Folder link. Other iSeries Access for Web users can also send items to your personal folder. The following types of items can be sent to a personal folder:

- SQL output generated by Run SQL
- PDF output created from Printer output
- Command completion status generated by Run Command (can only be sent to the user's own personal folder)

You can configure My Folder to send you e-mail notifications when new items are added to your personal folder. The My Folder link in the navigation pane also has an icon to indicate when the personal folder contains any items, and an icon to indicate when the personal folder contains new unopened items.

List installed software products

View the currently installed software products and software fix information for each software product on your iSeries server. A link to this information is provided from About iSeries Access for Web.

List system values

View the current system values on your iSeries server. A link to this information is provided from About iSeries Access for Web.

License Information

iSeries Access for Web is a licensed program. All components of iSeries Access for Web require an iSeries Access (5722-XW1) license before you can use them.

Important:

For V5Rx servers, a software license key is required for iSeries Access 5722-XW1. iSeries Access is included on the V5Rx Keyed Stamped Media that comes with all OS/400® V5Rx software orders. You receive a license key if you order 5722-XW1. If you have not ordered 5722-XW1, you may evaluate the product from the keyed stamped media for 70 days. At the end of the 70-day evaluation period, the product will be disabled if you have not ordered the product and received a software license key. The software license key is an 18-digit authorization code that allows the software product and feature on the keyed stamped media to be used on a specified iSeries server.

iSeries Access for Web is licensed by the number of concurrently active HTTP sessions to the iSeries server. The behavior of sessions is dependent on the implementation of the browser being used. For example, each new instance of Internet Explorer results in a new session, thus a new, unique license is used for each instance of Internet Explorer. Each new instance of Netscape Navigator uses the same session, therefore, only one license is used. iSeries Access for Web prompts for login at the start of each new session, so it is a good assumption that each time a login prompt appears, a new license is being requested.

iSeries Access for Web expires licenses at five minute intervals. A session that is idle for more than five minutes will have its license released. Activity (retrieving a new web page) after the license has expired will result in a new license being used. For example, when a user uses iSeries Access for Web to request some data from the iSeries, a license is retrieved and "held" by the session. If the browser is then left idle for five to ten minutes, the license being used for the session will be released. When another action is performed to the iSeries server from this browser, a new license is requested and used.

Note: Only activity to the iSeries server would result in a license being used. Browsing other web sites in the same browser window would not result in a new license being requested.

Licensing is managed at the iSeries Access (5722-XW1) level, not at the individual client level. Therefore, any combination of the iSeries Access for Windows® clients and iSeries Access for Web clients is allowable up to the license limit. Customers who acquire iSeries Access licenses are entitled to use the iSeries Access for Windows and iSeries Access for Web clients in any combination.

To determine the iSeries Access family usage limit:

1. Type the WRKLICINF command on the iSeries server to which you intend to connect. A list of products appears.
2. Type a 5 in the entry field next to the product 5722XW1. This will display the details for the iSeries Access family license product, including the usage limit. The usage limit should be equal to the number of licenses that are purchased for the iSeries Access family. Any number exceeding the purchased limit violates the IBM license agreement.

Chapter 2. iSeries Access for Web Setup Checklist

Use this checklist to guide you through the steps necessary to install, verify, and configure a simple iSeries Access for Web environment. These steps do not take into account other web applications or more complex web environments.

- 1. Verify your iSeries server has the necessary hardware listed in the “iSeries Server Hardware Requirements” on page 11.
 - 2. Verify your iSeries server has the prerequisite software listed in the “iSeries Server Software Requirements” on page 12.
 - 3. Verify your web browser meets the requirements listed in “Web Browser Requirements” on page 14.
 - 4. If the beta release of iSeries Access for Web was installed on your server, it must be deleted before installing V5R2 iSeries Access for Web. For details, see “Beta Release” on page 15.
 - 5. Install iSeries Access for Web on the iSeries server using the instructions in “Install iSeries Access for Web” on page 16.
 - 6. Now that the iSeries server software has been installed, install the latest program temporary fixes (PTFs) for the following:
 - Cumulative PTF package
 - Additional PTFs
 - WebSphere Application Server
 - ASF Tomcat/HTTP Server for iSeries
 - iSeries Access for Web
 - IBM WebSphere Host Publisher
- Refer to “Install PTFs” on page 16 for additional details.
- 7. Prepare for creating the HTTP Server using the information in “Preparation for creating the HTTP Server” on page 18.
 - 8. If you plan to use WebSphere 4.0, “HTTP setup for WebSphere 4.0” on page 19 contains details for:
 - Websphere administrative instances
 - Creating an HTTP server powered by Apache
 - Creating an original HTTP server
 - 9. Verify the web application server is set up and ready to be configured to run iSeries Access for Web for:
 - “WebSphere 4.0 Advanced Edition Environment” on page 22
 - “WebSphere 4.0 Advanced Single Server Edition” on page 22
 - “ASF Tomcat Server” on page 23

Note: V5R2 iSeries Access for Web (5722-XH2) does not support the IBM Websphere Application Server 3.5 environment. WebSphere 3.5 users should use V5R1 iSeries Access for Web (5722-XH1).

- 10. If you have V5R1 iSeries Access for Web installed, installing V5R2 iSeries Access has no impact on the V5R1 installation. See “Upgrade iSeries Access for Web to V5R2” on page 25 for more information.
 - 11. Configure iSeries Access for Web to run the web application server:
 - WebSphere Advanced Edition
 - WebSphere Advanced Single Server Edition
 - ASF Tomcat
- Refer to Appendix E, “CL Commands used with iSeries Access for Web” on page 117 for details.
- 12. If you plan to modernize existing server applications using Host Publisher, see “Install IBM Host Publisher 4.0” on page 27 for details.

-
- 13. The installation and configuration of iSeries Access for Web has completed. Follow “Verify the Installation” on page 29 to verify that iSeries Access for Web is installed and configured correctly and is operational.
-

iSeries Setup Considerations

- Some servers may need to be tuned to achieve optimal performance. Review the information on “Performance Tuning” on page 30.
- If you want to use the Document Library Services file system (QDLS), go to Appendix D, “Enrolling Users if You Use Document Library Services File System (QDLS)” on page 115. Skip this step if the server’s users were previously enrolled users for another client or if you do not access QDLS from the Files function.

For more information about iSeries Access for Web, see the references provided in Appendix A, “Sources of Information for iSeries Access for Web” on page 109.

WebSphere Setup Considerations

- iSeries Access for Web assumes that the WebSphere administrative server environment has been set up to use the QEJBSVR user profile. Using a user profile other than QEJBSVR is not supported. iSeries Access for Web defaults to use QEJBSVR.
- WebSphere tools such as Application Assembly Tool (ATT) must not be used to manage, manipulate, or change iSeries Access for Web installations and configurations.
- iSeries Access for Web will use the server-cfg.xml configuration file for the WebSphere Advanced Single Server Edition environment. If your WebSphere Advanced Single Server Edition environment is using a different configuration file, change the administrative server to use server-cfg.xml or create a new administrative server that does use this configuration file.

Part 2. iSeries Setup and Installation

Chapter 3. Install iSeries Access for Web on the iSeries server	11
iSeries Server Hardware Requirements	11
iSeries Server Software Requirements	12
Licensing Notes	13
Secure Sockets Layer (SSL) Notes	14
Web Browser Requirements	14
Netscape	14
Microsoft® Internet Explorer	15
Opera	15
Beta Release	15
Install iSeries Access for Web	16
Install PTFs	16
Preparation for creating the HTTP Server	18
Port	18
HTTP setup for WebSphere 4.0	19
WebSphere Administrative Servers	19
Create an HTTP server powered by Apache	19
Create an original HTTP server	21
WebSphere 4.0 Advanced Edition Environment	22
WebSphere 4.0 Advanced Single Server Edition	22
ASF Tomcat Server	23
IBM HTTP Server Powered by Apache Setup	23
ASF Tomcat setup	24
Upgrade iSeries Access for Web to V5R2	25
Configure iSeries Access for Web	25
WebSphere 4.0 Advanced Edition	26
WebSphere 4.0 Advanced Single Server Edition	26
ASF Tomcat	27
Install IBM Host Publisher 4.0	27
General information	27
Host Publisher Documentation	28
Verify the Installation	29
IBM HTTP Original and Apache Servers	29
WebSphere 4.0 Advanced Edition	29
WebSphere 4.0 Advanced Single Server Edition	30
iSeries Access for Web	30
Performance Tuning	30
Delete iSeries Access for Web and Host Publisher	31
Chapter 4. Security	33
General	33
Object Level Security	33
iSeries Access for Web Policies	33
Authentication	33
Using Exit Programs	33
Secure HTTP (HTTPS)	33
Configure an Original HTTP server to allow SSL	34
Configure an HTTP server powered by Apache	35
to allow SSL	35
Configure Digital Certificates	35
SSL port for WebSphere 4.0 Advanced Edition	36
SSL port for WebSphere 4.0 Advanced Single	36
Server Edition	36
SSL port for ASF Tomcat	37

Chapter 3. Install iSeries Access for Web on the iSeries server

You can install iSeries Access for Web on V5R1 and later OS/400 releases. If you are on an earlier release of OS/400, see the Upgrades topic in the Information Center for instructions on upgrading your OS/400 to a supported release. If you need to install a new release of OS/400, be sure to follow the instructions in the Install the OS/400 release topic in the Information Center before you continue installing iSeries Access for Web.

Note: In order to configure the iSeries server, you need a security level of Security Officer (*SECOFR). This is the highest level of security on the iSeries server. This security level is required for installation and configuration only, not for regular use of iSeries Access for Web.

iSeries Server Hardware Requirements

The tables below contain the recommended minimum requirements for server hardware. Servers not meeting these recommended minimum requirements may be used in environments that support a limited number of users, and that can tolerate longer server initialization.

Note: For help with sizing all system configurations, use the IBM Workload Estimator for iSeries at:
<http://www.ibm.com/eserver/iseries/support/servlet/EstimatorServlet>

Table 1. Server models

Server type	Processor feature
AS/400e™ Server 170	2292
AS/400e Server 720	2061
iSeries Model 270	2250
iSeries Model 820	2395

Table 2. Server memory

Memory amount	Comment
512 MB	Minimum
1 GB	Recommended

Table 3. Server disk space

Disk space required	Software product
170 MB	iSeries Access for Web

For instructions on how to check the amount of storage your server has available, see the Installing the OS/400 release topic in the Information Center at:
<http://www.ibm.com/eserver/iseries/infocenter>.

iSeries Server Software Requirements

iSeries Access for Web can be installed on iSeries servers running V5R1 and later OS/400 releases.

The tables below list the software required for using iSeries Access for Web in the IBM WebSphere Application Server and ASF Tomcat web application serving environments.

Note: Install each product at the latest level.

WebSphere Application Server environment

Table 4. Required software products for WebSphere 4.0 Application Server environment

Product	Option	Description
5722-SS1		Operating System/400 Version 5 Release x
5722-SS1	3	OS/400-Extended Base Directory Support
5722-SS1	8	OS/400- AFP Compatibility Fonts
5722-SS1	12	OS/400-Host Servers
5722-SS1	30	OS/400-QShell Interpreter
5722-SS1	34	OS/400-Digital Certificate Manager Note: This is required only to use the Secure Sockets Layer (SSL) protocol. See Secure Socket Layer (SSL) Notes for more information.
5722-IP1	Base	IBM Infoprint Server
5722-JV1	Base	Java Developer Kit
5722-JV1	3	Java Developer Kit Version 1.2
5722-JV1	5	Java Developer Kit Version 1.3
5722-JC1	Base	Toolbox for Java
5722-TC1	Base	TCP/IP Connectivity Utilities
5722-DG1	Base	IBM HTTP Server
• 5722-AC2 • 5722-AC3	• 56-bit • 128-bit	• Crypto Access Provider 56-bit for iSeries • Crypto Access Provider 128-bit for iSeries Note: This is required only to use the Secure Sockets Layer protocol. See Secure Socket Layer (SSL) Notes for more information.
5722-XW1	• Base • Option 1	• iSeries Access • iSeries Access Enablement Support Note: See Licensing Notes for more information.
• 5733-WS4 • 5733-WA4	• Base • Option 1	• IBM WebSphere Application Server Advanced Single Server Edition • IBM WebSphere Application Server Advanced Edition Note: A minimum fix level of 4.0.2 is required. See Installing PTFs for more information.

ASF Tomcat

Table 5. Required software products for ASF Tomcat environment

Product	Option	Description
5722-SS1		Operating System/400 Version 5 Release x
5722-SS1	3	OS/400-Extended Base Directory Support
5722-SS1	8	OS/400-AFP Compatibility Fonts
5722-SS1	12	OS/400-Host Servers
5722-SS1	30	OS/400-Qshell Interpreter
5722-SS1	34	OS/400-Digital Certificate Manager Note: This is required only to use the Secure Sockets Layer (SSL) protocol. See Secure Socket Layer (SSL) Notes for more information.
5722-IP1	Base	IBM Infoprint Server
5722-JV1	Base	Java Developer Kit
5722-JV1	3	Java Developer Kit Version 1.2
5722-JV1	5	Java Developer Kit Version 1.3 Note: This option is required only for Arabic language users.
5722-JC1	Base	Toolbox for Java
5722-TC1	Base	TCP/IP Connectivity Utilities
5722-DG1	Base	IBM HTTP Server
• 5722-AC2 • 5722-AC3	• 56-bit • 128-bit	• Crypto Access Provider 56-bit for iSeries • Crypto Access Provider 128-bit for iSeries Note: Only one of the above may be installed. Note: This is required only to use the Secure Sockets Layer protocol. See Secure Socket Layer (SSL) Notes for more information.
5722-XW1	• Base • Option 1	• iSeries Access • iSeries Access Enablement Support Note: See Licensing Notes for more information.

Licensing Notes

- iSeries Access for Web retrieves its license information from the 5722-XW1 Base and Option 1 software product. The XW1 product must be installed if you plan to use iSeries Access for Web.
- To update the usage limit for the 5722-XW1 product on your server, follow these steps:
 1. Type the WRKLICINF command on the iSeries server to which you intend to connect. A list of products appears.
 2. Type 2 in the entry field next to the product 5722XW1 V5, Feature 5050. Change the usage limit to the number of licenses that you have purchased for iSeries Access. If you have purchased the processor-based option for iSeries Access, enter the value *NOMAX for usage limit. Entering any number that exceeds the purchased limit violates the IBM license agreement.
 3. Enter the license key information by following these steps:
 - a. Type the WRKLICINF command on the iSeries server to which you intend to connect. A list of products appears.
 - b. Type 1 in the entry field next to the product 5722XW1 Option 1, Feature 5101. Enter the license key information.

Secure Sockets Layer (SSL) Notes

Secure Sockets Layer (SSL) is supported with iSeries Access for Web. To use SSL, order and install the appropriate iSeries software. You are responsible for making sure that you are using the correct encryption for your country or region and the countries or regions that your iSeries server does business in. Consult the following table for information on SSL software requirements:

Table 6. SSL Encryption Software Requirements

If you want	For V5Rx servers, install
56-bit server encryption	<ul style="list-style-type: none">• 5722-AC2, Cryptographic Access Provider 56-bit for AS/400.• 5722-SS1, OS/400 Option 34, OS/400-Digital Certificate Manager.• 5722-DG1, IBM HTTP Server.
128-bit server encryption	<ul style="list-style-type: none">• 5722-AC3, Cryptographic Access Provider 128-bit for AS/400.• 5722-SS1, OS/400 Option 34, Digital Certificate Manager.• 5722-DG1, IBM HTTP Server.

Web Browser Requirements

The following browsers have been tested with iSeries Access for Web:

- Netscape 4.7 (AIX®, Linux) and 6.2 (Windows)
- Internet Explorer 6.0 (Windows)
- Opera 5.0 (Linux) and 6.0 (Windows)

Other browsers (for these and other platforms) that support the current HTTP and HTML specifications should work, but have not been tested with iSeries Access for Web.

See the following for specific browser requirements:

Netscape

Cookies

iSeries Access for Web requires that the web browser allow cookies. The cookie configuration option should be set to one of the following:

- Accept all cookies
- Accept only cookies that get sent back to the originating server

Note: If your version of the browser does not have these specific options, ensure that the browser will allow/accept cookies.

To verify or modify your cookie configuration for Netscape 4.7, follow these steps:

1. Open your browser.
2. Select the **Edit** pull down menu.
3. Select the **Preferences** menu option.
4. Select the **Advanced** category.
5. The cookie options will be displayed.

To verify or modify your cookie configuration for Netscape 6.2, follow these steps:

1. Open your browser.
2. Select the **Edit** pull down menu.
3. Select the **Preferences** menu option.

4. Double-click the **Privacy & Security** category.
5. Select the **Cookies** category.
6. The cookie options will be displayed.

Microsoft® Internet Explorer

Cookies

iSeries Access for Web requires that the web browser allow cookies. The cookie configuration option should be set to: Allow per-session cookies (not stored).

Note: If your version of the browser does not have this specific option, ensure that the browser will allow/accept cookies.

To verify or modify your cookie configuration, follow these steps:

1. Open your browser.
2. Select the **Tools** pull down menu.
3. Select the **Internet Options** menu option.
4. Select the **Privacy** tab.
5. The cookie options will display.

Opera

Cookies

iSeries Access for Web requires that the web browser allow cookies. The cookie configuration option should be set to one of the following:

- Display received cookies.
- Accept only cookies from selected servers.
- Accept all cookies .

To verify or modify your cookie configuration, follow these steps:

1. Open your browser.
2. Select the **File** pull down menu.
3. Select the **Preferences** menu option.
4. Select the **Privacy** item.
5. The cookie options should be displayed.

Beta Release

Prior to the release of V5R2 iSeries Access for Web, the software product was available as a beta release.

The beta release must be deleted from the iSeries server before installing the official release of iSeries Access for Web. To remove the beta release, follow these steps:

1. Sign on to the server.
2. Use the QIWA2/RMVACCWEB2 command to remove the configuration information from the web application servers.

Note: If you do not recall what was configured, the /QIBM/UserData/Access/Web2/config/instances.properties file contains a listing of what web applications servers and instances were configured. Use the values listed in instances.properties as input to the RMVACCWEB2 command.

3. Run the following command DLTLCICPGM LICPGM(5722XH2)
4. Delete the directory /QIBM/UserData/Access/Web2

5. Verify the directory /QIBM/ProdData/Access/Web2 does not exist. Delete it if it does.
6. If iSeries Access for Web was configured for WebSphere Advanced Single Server Edition, the WebSphere subsystem should be ended and restarted to remove any configuration information that may be loaded in memory. To end the subsystem, run the command
ENDSBS SBS(QEJBAES4)
7. If iSeries Access for Web was configured for Tomcat, the Tomcat server should be ended and restarted to remove any configuration information that may be loaded in memory.

Install iSeries Access for Web

Installing iSeries Access for Web (5722-XH2) will create the required library (QIWA2), set up the directory structure in the integrated file system, and copy the files from the installation media to your V5Rx server.

Follow these steps to install iSeries Access for Web on the server:

1. Sign on to the iSeries server with *SECOFR authority.
2. Load the medium containing the licensed programs on the installation device. If the licensed programs are contained on more than one medium, you can load any one of them.
3. Type RSTLICPGM in the iSeries command prompt, then F4 to prompt the command.
4. Specify the following values on the Install Options display and press Enter:

Table 7. Licensed program install values

Parameter name	Parameter Key	Value
Product	LICPGM	5722XH2
Device	DEV	OPT1 is an example
Optional part to be restored	OPTION	*BASE

The licensed program will now install. If the licensed program is on multiple volumes, the install program will prompt you for a new volume. Load the next media volume, press G and then Enter. If you do not have any additional media volumes, press X and then Enter.

Notes:

1. If V5R1 iSeries Access for Web (5722-XH1) is already installed on the server, installing V5R2 iSeries Access for Web (5722-XH2) will not impact the V5R1 installation. V5R1 and V5R2 iSeries Access for Web can coexist on the server. For more information, see Upgrading iSeries Access for Web to V5R2.
2. After the installation of iSeries Access for Web, 5722-XH2 iSeries Access for Web will be listed as an installed licensed program. You can view the list using the server command GO LICPGM and selecting option 10.
3. The installation of iSeries Access for Web will not perform any configuration or start any jobs on the server. The configuration of iSeries Access for Web will be completed using the CFGACCWEB2 command. For more information on configuration, see “Configure iSeries Access for Web” on page 25.

Install PTFs

After the required software has been installed on the server, the latest available fixes should also be loaded and applied.

Cumulative PTF package

You should install the currently available cumulative PTF package for the OS/400 version you are running before installing any other fixes.

You must install the latest OS/400 cumulative PTF package before installing the group PTF for either WebSphere Application Server or ASF Tomcat.

Additional PTFs

The following PTFs may not be included in the OS/400 cumulative PTF package and should be installed.

Table 8. Additional PTFs

Product	PTF number
5722SS1	SI02028
5722SS1	SI01946
5722SS1	SI02756
5722DG1	SI02940

WebSphere Application Server

WebSphere PTFs are delivered as group PTFs. These group PTFs contain all the fixes required, across different software products, to bring WebSphere up to a specific fix level.

Select PTFs from the WebSphere web site:

<http://www.ibm.com/eserver/iseries/software/websphere/wsappserver>

Follow the links appropriate for your version of OS/400 and WebSphere.

Note: iSeries Access for Web requires a minimum fix level of 4.0.2.

ASF Tomcat/HTTP Server for iSeries

The ASF Tomcat web application server is part of the IBM HTTP Server for iSeries (5722-DG1) product. ASF Tomcat PTFs are delivered within the IBM HTTP Server for iSeries Group PTFs. These Group PTFs contain all the fixes required to bring the HTTP Server up to a specific fix level.

Select PTFs from the HTTP Server web site:

<http://www.ibm.com/servers/eserver/iseries/software/http>

Follow the links appropriate for your version of OS/400.

iSeries Access for Web

iSeries Access for Web Service Pack PTF information can be found on the web site for iSeries Access for Web:

<http://www.ibm.com/eserver/iseries/access/web/servicepacks.htm>

IBM WebSphere Host Publisher

Host Publisher is a separate product bundled with 5722-XH2 iSeries Access for Web.

Software fixes and instructions for loading and applying those fixes can be downloaded from the Host Publisher Web site:

<http://www.ibm.com/software/webservers/hostpublisher/>

Use the Support option to locate available information and fixes.

Before installing Host Publisher PTFs, be sure to install the product. Refer to the iSeries Setup Checklist for information about installing Host Publisher.

Preparation for creating the HTTP Server

Before creating the HTTP server, you must determine which port the HTTP server will use.

Port

When an HTTP server is running, it listens on a specific port servicing requests for information. When a request for information comes in through the port, the HTTP server will route the request to the configured web application server.

When you configure an HTTP server, you can use the default port number of 80, or you can specify a port number. Using a port other than the default offers some control of access and allows the administrator to isolate what requests are serviced through the HTTP server.

When using the default port number, the URL may look like `http://<server_name>/webaccess/iWAHome`. When using a port number other than the default, the port must be specified in the URL. It may look like `http://<server_name>:12345/webaccess/iWAHome`.

If you plan to use the default port, leave the port number information blank during the HTTP server creation and the default port will be used. See the information below if you plan to use a port other than the default.

Selecting a port other than the default

The information below will step you through the creation of an HTTP server that uses a port number other than the default. For the purpose of illustration, the following ports will be used:

- 2012 for the WebSphere Advanced Edition environment
- 2014 for the WebSphere Advanced Single Server Edition environment
- 2016 for the ASF Tomcat environment

If you prefer different port numbers or if these ports are already in use, use ports appropriate to your circumstances.

Before configuring the HTTP server, you should verify the port to be used is not already being used by another application. Follow the steps below to determine if the port is available:

1. Sign on to your server.
2. Run the command `CFGTCP`
3. Select the option to **Configure Related Tables**.
4. Select the option to **Work with Service Table Entries**.
5. Page through the list of configured services and determine if ports 2012, 2014 and 2016 (or the port you prefer) are already in use. If they are already in use, make note of a port not configured for use.
6. **Exit** the `CFGTCP` command.
7. Run the command `NETSTAT *CNN`.
8. Page through the list of ports currently in use and determine if the ports 2012, 2014, and 2016 (or the port you prefer) are already being used. If they are already in use, make note of a port not configured for use.

HTTP setup for WebSphere 4.0

The information in this section guides you through the creation of an HTTP server for WebSphere to use with iSeries Access for Web.

If you already have an HTTP server configured for use with WebSphere, review this information and verify your HTTP server settings.

You can choose to create an HTTP server powered by Apache or an Original HTTP server.

WebSphere Administrative Servers

When WebSphere is installed, the installation process creates a default administrative server that web applications like iSeries Access for Web can be configured to run in.

You can create additional WebSphere administrative servers and then configure iSeries Access for Web for those servers. This would allow you to manage access to iSeries Access for Web at the WebSphere application server level. It also allows you to tune WebSphere for iSeries Access for Web without impacting other web applications that may be installed in that administrative server of WebSphere.

If you want to create a WebSphere administrative server, refer to the WebSphere documentation on creating administrative servers and create the administrative server now. The WebSphere documentation can be found at <http://www.ibm.com/servers/eserver/iseries/software/websphere/wsappserver>.

After the administrative server has been created, it should be started. Refer to the WebSphere documentation on how to start the administrative server.

Create an HTTP server powered by Apache

The following steps guide you through the creation of an HTTP server powered by Apache.

1. Sign on to your server.
2. Run the server command STRTCPSVR SERVER(*HTTP) HTTPSVR(*ADMIN)
3. Open your browser to http://<your_server_name>:2001/
4. Click IBM HTTP Server for iSeries.
5. Click Configuration and Administration ->Administration -> Create HTTP Server.
6. Select the **HTTP server (powered by Apache)** button, then select **Next**.
7. Enter a server name, then select **Next**.
8. Select the **No** button, then select **Next**.

If you are using WebSphere Advanced Edition, go to step 9. If you are using WebSphere Advanced Single Server Edition, go to step 10 on page 20.

9. To configure this HTTP server to work with WebSphere Advanced Edition:
 - a. Enter /QIBM/UserData/WebASAdv4/<was_instance>/<http_server_name> for the Server root field.
 - Replace <http_server_name> with the name you specified in step 7.
 - Replace <was_instance> with the name of the WebSphere administrative server created during your setup, or use default if using the default WebSphere administrative server. For more information, see "WebSphere Administrative Servers".

Select **Next**.

- b. Enter /QIBM/UserData/WebASAdv4/<was_instance>/<http_server_name>/htdocs for the Document root field.
 - Replace <http_server_name> with the name you specified in step 7 on page 19.
 - Replace <was_instance> with the name of the WebSphere administrative server created during your setup, or use default if using the default WebSphere administrative server. For more information, see “WebSphere Administrative Servers” on page 19.

Click **Next**.

- c. Enter 2012, or the number you prefer, for the port number. For more information, see “Preparation for creating the HTTP Server” on page 18.

Click **Next**.

Go to step 11.

10. To configure this HTTP server to work with WebSphere Advanced Single Server Edition:
 - a. Enter /QIBM/UserData/WebASAEs4/<was_instance>/<http_server_name> for the Server root field.
 - Replace <http_server_name> with the name you specified in step 7 on page 19.
 - Replace <was_instance> with the name of the WebSphere administrative server created during your setup, or use default if using the default WebSphere administrative server. For more information, see “WebSphere Administrative Servers” on page 19.

Click **Next**.

- b. Enter /QIBM/UserData/WebASAEs4/<was_instance>/<http_server_name>/htdocs for the Document root field.
 - Replace <http_server_name> with the name you specified in step 7 on page 19.
 - Replace <was_instance> with the name of the WebSphere administrative server created during your setup, or use default if using the default WebSphere administrative server. For more information, see “WebSphere Administrative Servers” on page 19.

Click **Next**.

- c. Enter 2014, or the number you prefer, for the port number. For more information, see “Preparation for creating the HTTP Server” on page 18.

Click **Next**.

11. On the Combined log files page, click **Next**.

12. Click **Finish**.

13. Click **Configure**.

14. Under the Dynamic Content list, select **WebSphere Application Server**.

If you are using WebSphere Advanced Edition, go to step 15. If you are using WebSphere Advanced Single Server Edition, go to step 16.

15. Select the **WebSphere version 4 Advanced** button.

Go to step 17.

16. Select the **WebSphere version 4 single server** button.

17. In the **WebSphere domain** drop down dialog, select the name of the WebSphere administrative server created during your setup, or use default if using the default WebSphere administrative server. For more information, see “WebSphere Administrative Servers” on page 19. Click **Apply**.

18. Click **OK**.

19. The HTTP server configuration is complete, close the browser.

20. Run the server command
`STRTCPSVR SERVER(*HTTP) HTTPSVR(<http_server_name>)`
 Replace <http_server_name> with the name specified in step 7 on page 19.

Create an original HTTP server

The following steps will guide you through the creation of an original HTTP server.

1. Sign on to your server.
 2. Run the server command `STRTCPSVR SERVER(*HTTP) HTTPSVR(*ADMIN)`
 3. Open your browser to `http://<your_server_name>:2001/`
 4. Click **IBM HTTP Server for iSeries**.
 5. Click **Configuration and Administration -> Administration -> Create HTTP Server**.
 6. Select the **HTTP server (original)** button, then click **Next**.
 7. Enter a server name, then click **Next**.
 8. Select the **Create a new original type configuration** button, then click **Next**.
 9. Enter 2012 or 2014 for the port number, or the port number determined during your preparation. For more information, see “Preparation for creating the HTTP Server” on page 18. Click **Next**.
 10. Leave the default value in the Directory field, click **Next**.
 11. Click **Finish**.
 12. Click **Configure -> Java servlets**.
- If you are using WebSphere Advanced Edition, go to step 13. If you are using WebSphere Advanced Single Server Edition, go to step 14.
13. Select the **WebSphere version 4 Advanced** button.
 Go to step 15.
 14. Select the **WebSphere version 4 single server** button.
 15. In the **WebSphere domain** drop down dialog, then select the name of the WebSphere administrative server created during your setup, or use **default** if using the default WebSphere administrative server. For more information, see “WebSphere Administrative Servers” on page 19. Click **Apply**.
 16. The HTTP server configuration is complete, close the browser.
 17. Run the server command
`STRTCPSVR SERVER(*HTTP) HTTPSVR(<http_server_name> '-nolastmod')`.
 Replace <http_server_name> with the name specified in step 7.

Note: The `-nolastmod` parameter in the above server command makes the web browser work properly when communicating with an Original HTTP server on an iSeries server. If you prefer to not have to specify the parameter, you can add a directive to the HTTP server configuration. To add the directive to the HTTP server configuration:

- a. Sign on to the server.
- b. Run the server command `WRKHTTPCFG` to open the HTTP server configuration file.
- c. Add `LastMod Off` to the configuration and save the changes.
- d. Run the server command
`ENDTCPSVR SERVER(*HTTP) HTTPSVR(<http_server_name>)`.
- e. Run the server command
`STRTCPSVR SERVER(*HTTP) HTTPSVR(<http_server_name>)`.

WebSphere 4.0 Advanced Edition Environment

The steps below will help you verify WebSphere 4.0 Advanced Edition is set up for iSeries Access for Web.

1. Sign on to your server.
2. Run the server command WRKACTJOB SBS(QEJBADV4)

The subsystem should be displayed and the following jobs should be listed:

- QEJADMIN
- QEJBMNTR

Notes:

- a. If the subsystem is not running, run the server command STRSBS QEJBADV4/QEJBADV4
- b. If you created a WebSphere administrative server and started it in "WebSphere Administrative Servers" on page 19, an ADMIN job and a MNTR job should also be listed for the administrative server you created. If they are not listed, you need to start your administrative server now.
3. The HTTP Server set up steps had you create an HTTP server using port 2012 (or one you prefer). If you are using a port other than the default port 80, the WebSphere alias table must be updated. To update the WebSphere alias table:
 - a. Open the WebSphere Administrative Console on your Windows NT® or Windows 2000 workstation to the WebSphere administrative server being used.
 - b. Under the WebSphere Administrative Domain, click **Virtual Hosts**.
 - c. On the General tab, there is a table of Host Aliases listed. You need to add the 2012 port (or the one you specified in the HTTP configuration) to the list. Click **Apply**.
 - d. Expand **Nodes** under the WebSphere Administrative Domain. Right-click on your node/server name, then click **Regen Webserver Plugin**.
4. Restart your WebSphere administrative instance using the WebSphere Administrative console. To restart your WebSphere administrative instance:
 - a. Right-click on your node/server name and click **Stop**.

Note: Do not run the server command ENDSBS QEJBADV4 to end WebSphere unless all the jobs under it have ended.

- b. Run the server command WRKACTJOB SBS(QEJBADV4)
- c. When the ADMIN/MNTR jobs for your administrative instance end, restart your administrative server. For information on administrative servers, see "WebSphere Administrative Servers" on page 19.

WebSphere 4.0 Advanced Single Server Edition

The steps below will help you verify WebSphere 4.0 Advanced Single Server Edition is setup for iSeries Access for Web.

1. Sign on to your server.
2. Run the server command WRKACTJOB SBS(QEJBAES4)

Notes:

- a. If the subsystem is not running, run the server command STRSBS QEJBAES4/QEJBAES4
- b. If you created a WebSphere administrative server and started it in "WebSphere Administrative Servers" on page 19, a job should also be listed for the administrative server you created. If it is not listed, start your administrative server now.
3. Add a property value to the WebSphere default server's JVM settings by:

- a. Open the web-based WebSphere Administrative Console using the port you specified when you created the administrative server. Open the default administrative console using `http://<server_name>:9090/admin/`
 - b. Log in to the console.
 - c. Expand **Nodes -> your_node/server_name -> Application Servers -> Default Server -> Process Definition.**
 - d. Click **JVM Settings**.
 - e. Page down to Advanced Settings and click **System Properties**.
 - f. Click **New**.
 - g. In the **Name** field, enter `client.encoding.override`
 - h. In the **Value** field, enter `iso-8859-1`
 - i. Click **OK**
 - j. At the top of the page, click **Configuration needs to be saved**. Click **OK**.
 - k. Click **Exit** to exit the console. **Do not** just close the browser to exit the console.
 - l. If you configured your HTTP server to use the default port of 80 (instead of 2014 or a port number you prefer), go to 5.
4. The HTTP Server setup steps had you create an HTTP server using port 2014 (or one you prefer). If you are using a port other than the default port 80, the WebSphere alias table must be updated. To update the WebSphere alias table:
 - a. Open the web-based WebSphere Administrative Console using the port you specified when you created the administrative server. The default administrative server console can be opened using
`http://<server_name>:9090/admin/`
 - b. Login to the console.
 - c. Expand **Virtual Hosts -> default_host**.
 - d. Click **Aliases**.
 - e. Click **New** to add 2014 (or the port you specified in the HTTP configuration) to the list of aliases.
 - f. After adding the port number, click **Plugin configuration needs to be regenerated**.
 - g. Click **Generate**.
 - h. When a blank page is displayed, click **Save** and save the configuration.
 - i. Click **Exit** to exit the console. **Do not** just close the browser.
 5. Run the server command ENDSBS QEJBAES4 to end the WebSphere subsystem. Wait for the subsystem to end.
 6. To start the subsystem, run the server command STRSBS QEJBAES4/QEJBAES4

ASF Tomcat Server

The steps below will help you set up an IBM HTTP Server powered by Apache and Apache Software Foundation (ASF) Tomcat web application server.

IBM HTTP Server Powered by Apache Setup

Use these steps to set up an Apache powered IBM HTTP Server for a Tomcat web application server:

1. Sign on to your server.
2. Run the server command STRTCPSVR SERVER(*HTTP) HTTPSVR(*ADMIN)
3. Open your browser to `http://<your_server_name>:2001/`
4. Click **IBM HTTP Server for iSeries**.
5. Click **Configuration and Administration -> Administration -> Create HTTP Server**.
6. Select the **HTTP server (powered by Apache)** button, then click **Next**.
7. Enter a server name; then click **Next**.
8. Select the **No** button; then click **Next**.

9. Leave the default value for Server root; then click **Next**.
10. Leave the default value for the Document root; then click **Next**.
11. Enter a port number.

Note: For the purpose of illustration, this document will use port 2016. If you plan to use 2016, or any other port other than the default port 80, see the information on ports under “Preparation for creating the HTTP Server” on page 18 to verify that the port that you plan to use is not already in use.

- Click **Next**.
12. Under Combined log files, click **Next**.
 13. Click **Finish**.
 14. Click **Configure**.
 15. Under Dynamic Content, click **ASF Tomcat Settings**.
 16. Select the **Enable servlets for this HTTP Server** check box.
 17. Deselect the **Enable an "in-process" servlet engine** check box.
 18. Select the **Enable "out-of-process" servlet engine connections** check box.
 19. Click **Add** for Out-of-process workers. In the Add dialog:
 - a. Change the default port of 8009 to an available port number. Use the information on ports under “Preparation for creating the HTTP Server” on page 18 to determine an available port. Make note of the port number for use when configuring “ASF Tomcat” on page 27.
 - b. In the URLs field, add /webaccess/*
 - c. Click **Continue**. Ignore any error messages that may be displayed.
 - d. Click **OK**.
 20. You do not need to start the HTTP server at this time.
 21. Go to the ASF Tomcat setup procedure.

ASF Tomcat setup

Use these steps to setup an ASF Tomcat web application server:

1. Sign on to the server
2. Run the server command STRTCPSVR SERVER(*HTTP) HTTPSVR(*ADMIN).
3. Open your browser to http://<your_server_name>:2001/
4. Click **IBM HTTP Server for iSeries**.
5. Click **Configuration and Administration**.
6. Click **ASF Tomcat -> Create ASF Tomcat Server**.
7. Enter an ASF Tomcat server name. It can be the same name you used to create the HTTP Apache server in step 7 on page 23 of “IBM HTTP Server Powered by Apache Setup” on page 23. Click **Next**.
Make note of the following fields, you will need the values when you “Configure iSeries Access for Web” on page 25:
 - Server userid
 - ASF Tomcat home directory

Note: In the Java version (JDK) field, Arabic language users should select version 1.3.

8. Click **Next**.
9. Change the 8009 port number to that which was specified in step 19 of “IBM HTTP Server Powered by Apache Setup” on page 23. Click **Next**.
10. Under Application Contexts, click **Add**.
11. Enter /webaccess for the URL path. Enter webapps/webaccess for the Application base directory.
12. Click **Continue** and ignore any error messages.
13. Click **Next**.

14. Click **Finish**. You do not need to start the Tomcat web server at this time.
Close the browser.
-

Upgrade iSeries Access for Web to V5R2

If V5R1 iSeries Access for Web (5722-XH1) was already installed on your server, installing V5R2 iSeries Access for Web (5722-XH2) had no impact on the V5R1 installation. V5R1 and V5R2 iSeries Access for Web can coexist on the server.

To understand the differences between the V5R1 and V5R2 versions of iSeries Access for Web, see “What’s New for V5R2” on page 3.

When V5R2 iSeries Access for Web is installed, the installation process does not make any changes to V5R1 iSeries Access for Web nor will it query or copy any web application server configuration information.

When V5R2 iSeries Access for Web is configured using the CFGACCWEB2 command, the following actions automatically occur the first time the command is run:

- V5R1 iSeries Access for Web user generated data will be copied to the V5R2 iSeries Access for Web directory structure.
- The V5R1 iSeries Access for Web policy information will be copied to the V5R2 iSeries Access for Web configuration.
- The V5R1 iSeries Access for Web file content-type (MIME-type) mappings will be copied to the V5R2 iSeries Access for Web configuration.

To prevent iSeries Access for Web from automatically copying the previous release’s information, perform the following before running the CFGACCWEB2 command:

1. Create the file/QIBM/UserData/Access/Web2/config/migration.properties.
 2. Using an editor, add `was35migrationrun=true` to the migration.properties file.
-

Configure iSeries Access for Web

When iSeries Access for Web was installed several CL commands were installed to library QIWA2. These commands should be used to perform actions such as configuring, starting, ending, and removing the iSeries Access for Web configuration within the web application sever.

The iSeries Access for Web CL commands are:

- CFGACCWEB2 - Configure the iSeries Access for Web application server.
- STRACCWEB2 - Start the iSeries Access for Web application server.
- ENDACCWEB2 - End the running iSeries Access for Web application server.
- RMVACCWEB2 - Remove the iSeries Access for Web application server configuration.

The information below will step you through configuring iSeries Access for Web within the web application server, and then starting iSeries Access for Web.

Only the CFGACCWEB2 and STRACCWEB2 commands are used to configure and start iSeries Access for Web. For more information on using all the iSeries Access for Web CL commands, see Appendix E, “CL Commands used with iSeries Access for Web” on page 117.

WebSphere 4.0 Advanced Edition

Use these steps to configure iSeries Access for Web for WebSphere 4.0 Advanced Edition:

1. Sign on to your server.
2. Run the server command STRSBS QEJBADV4/QEJBADV4 and start your administrative server if using an administrative server other than the default.
3. Run the server command WRKACTJOB SBS(QEJBADV4).
4. Enter 5 on QEJBADMIN, or the admin job for your administrative server.
5. Enter 10 and verify the Ready message is displayed.
6. Run the server command
`QIWA2/CFGACCWEB2 APPSVRTYPE(*WAS40ADV) PORT(<xxxxx>)
WASINST('<was_instance_name>')`

Notes:

- a. <xxxxx> is a port number used by the iSeries Access for Web web container that gets created in the WebSphere configuration. This is a different port number than any of the others previously mentioned. This port number must be unique and unused. See "Preparation for creating the HTTP Server" on page 18 for information on determining available port numbers.
- b. <was_instance_name> is the name of the WebSphere administrative server you are using. If you are using the default WebSphere administrative server, specify *DEFAULT. For information on administrative servers, see "WebSphere Administrative Servers" on page 19.
7. Run the server command
`QIWA2/STRACCWEB2 APPSVRTYPE (*WAS40ADV) WASINST('<was_instance_name>').`

Note: <was_instance_name> is the name of the WebSphere administrative server that was just configured. If you are using the default WebSphere administrative server, specify *DEFAULT.

8. Run the sever command WRKACTJOB SBS(QEJBADV4). There should a job called ISERIESACC listed.
9. Open your browser to `http://<your_server_name>:2012/webaccess/iWAHome`. Be sure the case matches the example. The iSeries Access for Web home page should be displayed.

Note: The first call of the iWAHome page may take a few minutes, but subsequent calls should not take as long.

WebSphere 4.0 Advanced Single Server Edition

Use these steps to configure iSeries Access for Web for WebSphere 4.0 Advanced Single Server Edition:

1. Sign on to your server.
2. Run the server command ENDSBS QEJBAES4
3. Run the server command
`QIWA2/CFGACCWEB2 APPSVRTYPE(*WAS40SNG) WASINST('<was_instance_name>').`

Note: <was_instance_name> is the name of the WebSphere administrative server you are using. If you are using the default WebSphere administrative server, specify *DEFAULT. For information on administrative servers, see "WebSphere Administrative Servers" on page 19.

4. Run the server command STRSBS QEJBAES4/QEJBAES4.
5. Start your administrative server if using an administrative server other than the default.
6. Run the server command WRKACTJOB SBS(QEJBAES4).
7. Enter 5 on DEFAULT_SE job, or the job in your administrative server.

8. Enter 10 and verify the Ready message is displayed.
9. Open your browser to `http://<your_server_name>:2014/webaccess/iWAHome`
Be sure the case matches the example. The iSeries Access for Web home page should be displayed.

Note: The first call of the iWAHome page may take a few minutes, but subsequent calls should not take as long.

ASF Tomcat

Use these steps to configure iSeries Access for Web for ASF Tomcat:

1. Sign on to your server.
2. Run the server command

```
QIWA2/CFGACCWEB2 APPSVRTYPE(*ASFTOMCAT) TCSVRNAME(<tc_server_name>)
TCHOMEDIR('<tc_home_directory>') TCUSRPRF(<user_id>).
```

Notes:

- a. <tc_server_name> is the name of the ASF Tomcat server that was created to run iSeries Access for Web in “IBM HTTP Server Powered by Apache Setup” on page 23.
- b. <tc_home_directory> is the ASF Tomcat home directory that was specified in step 7 on page 24 of “ASF Tomcat setup” on page 24. You were asked to make note of this value.
- c. <user_id> is the Tomcat Server userid that was specified in step 7 on page 24 of “ASF Tomcat setup” on page 24. You were asked to make note of this value.
3. Run the server command `STRTCPSVR SERVER(*HTTP) HTTPSVR(*ADMIN)`.
4. Run the server command
`STRTCPSVR SERVER(*HTTP) HTTPSVR(<http_server_name>)`.

Note: Replace <http_server_name> with the name of the Apache powered IBM HTTP server that was created in step 7 on page 23 of “IBM HTTP Server Powered by Apache Setup” on page 23.

5. Open your browser to `http://<your_server_name>:2001/`
6. Click **IBM HTTP Server for iSeries**.
7. Click **ASF Tomcat -> Manage ASF Tomcat servers**.
8. Select the button for the Tomcat server that was created in “ASF Tomcat setup” on page 24, then click **Start**.
9. Run the server command `WRKACTJOB SBS(QSYSWRK)`
Page down through the list of jobs and verify the Tomcat server is listed as a running job. The Tomcat server job will have the same name as the Tomcat server you configured. Let the job run for a few minutes so it can initialize.
10. Open your browser to `http://<your_server_name>:2016/webaccess/iWAHome`. Be sure the case matches the example. The iSeries Access for Web home page should be displayed.

Note: The first call of the iWAHome page may take a few minutes, but subsequent calls should not take as long.

Install IBM Host Publisher 4.0

General information

Host Publisher is divided into two major components: Host Publisher (iSeries server side) and Host Publisher Studio.

Host Publisher Studio provides the development environment for creating Web applications. The server side provides the runtime environment for executing Web applications created with Host Publisher Studio. Using Host Publisher Studio, you can create Web-to-host applications, publish them to the server, and provide access to an end user.

Host Publisher, and Host Publisher Studio are bundled with 5722-XH2 iSeries Access for Web and are shipped on CD-ROM installation media.

The information below will direct you to the Host Publisher documentation that will guide you through the installation.

Note: After the installation of Host Publisher, "5724-B81 Host Publisher Server" will be listed on the server as an installed licensed program. You can view the list using the command GO LICPGM and selecting option 10.

Host Publisher Documentation

Host Publisher documentation consists of a Planning and Installation Guide for iSeries and an Administrator's and User's Guide.

Language

The root directory of the IBM WebSphere Host Publisher Server CD-ROM contains a directory called "OS400". Within the "OS400" directory are a number of directories that contain translated versions of the Planning and Installation Guide for iSeries and the Administrator's and User's Guide. The guides are available in PDF and HTML formats. The IBM WebSphere Host Publisher Server CD-ROM is in PC-DOS format. You can access the directories and files using your workstation.

Table 9. Language directories

Language	Path on CD-ROM
English	\OS400\en
Chinese (Simplified)	\OS400\zh
Chinese (Traditional)	\OS400\zh_TW
French	\OS400\fr
German	\OS400\de
Italian	\OS400\it
Japanese	\OS400\ja
Korean	\OS400\ko
Portuguese (Brazilian)	\OS400\pt_BR
Spanish	\OS400\es
Turkish	\OS400\tr

The documents are available in .html and .pdf formats. Within a directory listed in the above table, you can open the following files to view the documents listed:

Planning and Installation Guide

(Also available in the path /QIBM/ProdData/HostPublisher/doc/install after Host Publisher is installed to the iSeries server.)

- as4inst.pdf (Requires Adobe Acrobat Reader)
- as4inst.htm (Requires web browser)

Administrator's and User's Guide

(Also available in the path /QIBM/ProdData/HostPublisher/doc/guide after Host Publisher is installed to the iSeries server.)

- guide.pdf (Requires Acrobat reader)
- guide.htm (Requires web browser)

A Programmer's Guide and Reference

(Available in the path /QIBM/ProdData/HostPublisher/doc/proggd after Host Publisher is installed to the iSeries server.)

- progguid.pdf (Requires Acrobat reader)
- proggd.htm (Requires web browser)

Verify the Installation

The following steps will help you verify that all components of the web serving environment have been configured and are running so that iSeries Access for Web can be used.

IBM HTTP Original and Apache Servers

Use these steps to verify the installation of an IBM HTTP original or Apache server.

1. Sign on to the server
2. Run the server command WRKACTJOB SBS(QHTTPSVR)
3. Several jobs should be listed with the name of the HTTP server that was configured in either "Create an HTTP server powered by Apache" on page 19 or "Create an original HTTP server" on page 21.

Note: If the Original HTTP server has not been started, start it using the command

STRTCPSVR SERVER(*HTTP) HTTPSVR(<http_server_name> '-nolastmod').

If the HTTP server powered by Apache has not been started, start it using the command

STRTCPSVR SERVER(*HTTP) HTTPSVR(<http_server_name>).

WebSphere 4.0 Advanced Edition

To verify iSeries Access for Web has been configured within WebSphere:

1. Open the WebSphere Application Server administrative console on your Windows NT or Windows 2000 workstation.
2. Expand **WebSphere Administrative Domain -> Nodes -> your server's name -> Application Servers**.
3. iSeriesAccessforWeb should be listed under the Application Servers.

Note: If iSeriesAccessforWeb is not listed, use the QIWA2/CFGACCWEB2 command to configure iSeries Access for Web for WebSphere Advanced Edition.

To verify the iSeries Access for Web application server has been started:

1. Sign on to the server.
2. Run the server command WRKACTJOB SBS(QEJBADV4).

Note: If the subsystem is not running, start it using the command STRSBS QEJBADV4/QEJBADV4.

3. Verify that there is at least one job labeled ISERIESACC listed within subsystem.

Note: If ISERIESACC is not listed, use the QIWA2/STRACCWEB2 command to start iSeries Access for Web for WebSphere Advanced Edition.

WebSphere 4.0 Advanced Single Server Edition

To verify the iSeries Access for Web application server has been started:

1. Sign on to the server.
2. Run the server command WRKACTJOB SBS(QEJBAES4).

Note: If the subsystem is not running, start it using the command STRSBS QEJBAES4/QEJBAES4.

3. Verify that there is a job running within the subsystem for the WebSphere administrative server you configured in "WebSphere Administrative Servers" on page 19. If the administrative server is not running, start it now.

To verify iSeries Access for Web has been configured within WebSphere:

1. Open the WebSphere Application Server administrative console in your web browser. The default administrative server console can be opened at http://<your_server_name>:9090/admin/
2. Sign on to the WebSphere console.
3. Expand **Nodes -> your server's name -> Enterprise Applications**.
4. iSeriesAccessforWeb should be included in a list of installed applications. If it is not, use the QIWA2/CFGACCWEB2 command to configure iSeries Access for Web for WebSphere Advanced Single Server Edition.
5. iSeriesAccessforWeb should be in a running state. If it is not running, use the console to start it.

iSeries Access for Web

Use the following to verify the installation of iSeries Access for Web.

- If you configured the HTTP server to use the default port, open your browser to http://<server_name>/webaccess/iWAHome
- If you configured the HTTP server to use a port determined in "Preparation for creating the HTTP Server" on page 18, open your browser to http://<server_name>:<port>/webaccess/iWAHome

Performance Tuning

The workload required to support a web serving environment with WebSphere Application Server is greater than traditional workload environments. Your iSeries server may need to be tuned to operate efficiently for a web serving environment.

The following links will provide information to help tune the iSeries server for this environment:

- **IBM WebSphere Application Server for iSeries Performance Considerations**
<http://www.ibm.com/servers/eserver/iseries/software/websphere/wsappserver/product/PerformanceConsiderations.html>
- **iSeries performance capabilities guidelines documents**
<http://publib.boulder.ibm.com/pubs/html/as400/online/chgfrm.htm>
- **IBM Workload Estimator for iSeries**
<http://www.ibm.com/eserver/iseries/support/servlet/EstimatorServlet>

Delete iSeries Access for Web and Host Publisher

To delete iSeries Access for Web and Host Publisher from the server, follow these steps:

1. Sign on to the server.
2. Enter QIWA2/RMVACCWEB2 for all web application servers, and their instances, that were configured to run iSeries Access for Web. The RMVACCWEB2 command will remove the iSeries Access for Web configuration within the web application server.
3. Enter GO LICPGM, option 12.
4. If Host Publisher was installed, page down through the list of installed licensed programs and locate 5724-B81. Enter 4 to delete 5724-B81.
5. Page down through the list of installed licensed programs and locate 5722-XH2. Enter 4 to delete 5722-XH2.
6. Press Enter to delete the licensed program products.

Notes:

1. If the iSeries Access for Web configuration was removed from WebSphere Advanced Single Server Edition or ASF Tomcat, the WebSphere subsystem or Tomcat server should be restarted to remove any configuration information that may be loaded in the memory.
2. The following directories will not be deleted from the server:
 - /QIBM/UserData/Access/Web2
 - /QIBM/UserData/HostPublisher
3. See "Host Publisher Documentation" on page 28 for details on deleting Host Publisher from the iSeries server.

Chapter 4. Security

General

Object Level Security

iSeries Access for Web uses iSeries object level security when accessing objects and resources. Users will not be able to access objects and resources on the iSeries server if their user profile does not have the proper authority.

iSeries Access for Web Policies

iSeries Access for Web policies can be used to restrict user access to iSeries Access for Web functions. Policies can be managed for individual users and groups of users. iSeries user profiles and group profiles are used for policy management. See iSeries Access for Web Policies for more information on policies.

Authentication

iSeries Access for Web uses HTTP basic authentication to authenticate users. HTTP basic authentication encodes the user profile and password, but does not encrypt them. To ensure that the authentication information and data are encrypted, HTTPS (secure HTTP) should be used. See the following section for information on configuring HTTPS.

Using Exit Programs

iSeries Access for Web makes extensive use of the following iSeries Optimized Host Servers:

- Signon
- Central
- Remote Command/Program Call
- Database
- File
- Network Print

Exit programs that restrict access to these servers, especially Remote Command/Program Call, will cause all or portions of iSeries Access for Web to not function.

Secure HTTP (HTTPS)

The Internet was designed to be an open system and it allows any computer on the network to see the messages passing through. To consider an information transaction secure, it has to have the following characteristics:

Confidentiality

Use encryption if you want to ensure that the contents of the message remain private as they pass through the network.

Integrity

Use encryption and digital signatures if you want to ensure integrity. Messages are not altered while being transmitted.

Accountability

Use digital signatures when both the sender and the receiver agree that the exchange took place to ensure accountability.

Authenticity

OS/400 SSL provides server authentication so you can authenticate with whom you are talking.

You can configure the iSeries server to use a security protocol, called Secure Sockets Layer (SSL), for data encryption and client/server authentication. A client establishes an SSL session by sending an HTTPS request to the server on the SSL port. If SSL client authentication is enabled on the server, a client certificate is requested for any HTTPS request. SSL uses a handshake protocol where the server authenticates and the client authenticates if enabled. When authenticated, they agree on the security keys to use for the session, and the algorithms to be used for encryption and message digests or hashes. When a session has been established, all data exchanged on that session is encrypted.

Use this checklist to guide you through the steps for enabling HTTPS. The steps below are provided as a quick-start to help you get started using SSL. The steps may not address all issues relative to your environment.

- 1. If you are new to SSL, HTTPS, or digital certificates, review the following information before configuring SSL.
 - Security concepts information in the iSeries Information Center.
 - Security and SSL information in the HTTP server documentation at <http://www.ibm.com/servers/eserver/iseries/software/http>
- 2. Configure your HTTP server instance to allow SSL connections. You must already have created an HTTP server that you want to enable to run SSL. For information on creating an HTTP server, see “HTTP setup for WebSphere 4.0” on page 19.
 - “Configure an Original HTTP server to allow SSL”.
 - “Configure an HTTP server powered by Apache to allow SSL” on page 35.
- 3. Configure digital certificates through the Digital Certificate Manager. For more information, see “Configure Digital Certificates” on page 35.
- 4. Configure the web application server to use the SSL port.
 - “SSL port for WebSphere 4.0 Advanced Edition” on page 36.
 - “SSL port for WebSphere 4.0 Advanced Single Server Edition” on page 36.
 - “SSL port for ASF Tomcat” on page 37.
- 5. Open a browser to one of the following URLs:
 - If using the default SSL port of 443
https://<server_name>/webaccess/iWAHome
 - If using any other port number, replace the <port> with the port number configured with the HTTP server.
https://<server_name>:<port>/webaccess/iWAHome

Configure an Original HTTP server to allow SSL

To enable an original HTTP server instance configuration for SSL connections, do the following:

1. Sign on to your server.
2. Run the server command STRTCPSVR SERVER(*HTTP) HTTPSVR(*ADMIN)
3. Open a browser to http://<server_name>:2001
4. Click IBM HTTP Server for iSeries -> Configuration and Administration -> Administration -> Manage HTTP Servers.

5. From the list of configured HTTP servers, select the button for the HTTP server you wish to work with, then click **Stop**.
6. Click **Configure** button -> **Security configuration**.
7. Select the **Allow SSL connections** check box.
8. The SSL port field defaults to port number 443. You can use 443 as long as this port is not already in use by another HTTP server or application. You can also change this value to use a port that is not already in use. For information on determining port availability, see "Preparation for creating the HTTP Server" on page 18.
9. Click **Apply**.
10. The displayed page will be updated. Make note of the value updated in the Application ID field, you will need to know this for "Configure Digital Certificates".
11. Close the browser session.
12. Do not start the HTTP server at this time.

Configure an HTTP server powered by Apache to allow SSL

To enable an HTTP server powered by Apache instance configuration for SSL connections, do the following:

1. Sign on to your server.
2. Run the server command STRTCPSVR SERVER(*HTTP) HTTPSVR(*ADMIN)
3. Open a browser to `http://<server_name>:2001`
4. Click **IBM HTTP Server for iSeries -> Configuration and Administration -> Administration -> Manage HTTP Servers**.
5. From the list of configured HTTP servers, select the button for the HTTP server you wish to work with, then click **Stop**. Click **Configure**.
6. In the left pane, verify `<http_server_name> global settings` is selected.
7. Under Web Site Definition, click **General Settings**.
8. Page down to **Server IP address and port to listen on**. Select **Add**.
9. Enter **All** for the IP address.
10. Enter a port number. 443 is the default SSL port, but you can use any port number as long as that value is not already in use. For information on determining port availability, see "Preparation for creating the HTTP Server" on page 18. Click **Continue**. Click **OK**.
11. Under Web Site Definition, click **Context Management**.
12. Page down to **Virtual Host contexts**. Click **Add a virtual host**.
13. Enter `<your_server_name>:<port>` and click **Continue**. Click **OK**.

Note: Use the same port number used in step 10.

14. In the left pane, select **Virtual Host <your_server_name>:<port_number>**. The right pane will refresh.
15. Under Authentication and Security, click **SSL General Settings**.
16. Select the **Enable SSL** check box. Make note of the value in Application name field, you will need this value for "Configure Digital Certificates". Click **OK**.
17. Close the browser session.
18. Do not start the HTTP server at this time.

Configure Digital Certificates

The steps below assume that the *SYSTEM certificate store has been created and a certificate exists within the store. For information on setting up the certificate store, see the Security concepts information in the iSeries Information Center.

1. Sign on to your server.
2. Run the server command STRTCPSVR SERVER(*HTTP) HTTPSVR(*ADMIN)
3. Open a browser to `http://<server_name>:2001/`
4. Click **Digital Certificate Manager -> Select a Certificate Store**.

5. Select the ***SYSTEM** button. Click **Continue**.
6. Enter the Certificate store password. Click **Continue**.
7. Click **Manage Applications -> Update certificate assignment**.
8. Select the **Server** button. Click **Continue**.
9. Page down through the list of applications and locate the application for your HTTP server. The name is the value you were asked to make note of when you configured your original HTTP server for SSL in step 10 on page 35, or when you configured your HTTP server powered by Apache in step 16 on page 35. Select the button for your application.
10. Click **Update Certificate Assignment -> Assign New Certificate**.
11. Close the browser session.
12. Do not start the HTTP server at this time.

SSL port for WebSphere 4.0 Advanced Edition

The SSL port must be added to the WebSphere alias table. To update the WebSphere alias table, do the following:

1. Open the WebSphere Administrative Console on your Windows NT or Windows 2000 workstation to the WebSphere administrative instance being used.
2. Under the WebSphere Administrative Domain, click **Virtual Hosts**.
3. On the General tab, add your SSL port to the table of Host Aliases. Click **Apply**.
4. Under the WebSphere Administrative Domain, expand **Nodes**.
5. Right-click your node/server name, and click **Regen Webserver Plugin**.
6. Right-click on your node/server name, and click **Stop** to restart your WebSphere administrative server.

Note: Do not run the server command ENDSBS QEJBADV4 to end WebSphere unless all the jobs under it have ended.

7. Run the server command WRKACTJOB SBS(QEJBADV4)
8. When the ADMIN/MNTR jobs for your administrative instance end, restart your administrative server.
9. To start the HTTP server, run one of the following server commands:
 - For an Original HTTP server, run
STRTCPSVR SERVER(*HTTP) HTTPSVR(<http_server_name> '-nolastmod')
 - For an HTTP server powered by Apache, run
STRTCPSVR SERVER(*HTTP) HTTPSVR(<http_server_name>)

SSL port for WebSphere 4.0 Advanced Single Server Edition

The SSL port must be added to the WebSphere alias table. To update the WebSphere alias table, do the following:

1. Open the web-based WebSphere Administrative Console using
`http://<server_name>:9090/admin/`
Login to the console.
2. Expand **Virtual Hosts -> default_host**
3. Click **Aliases**.
4. Click **New** to add the SSL port to the list of aliases.
5. After adding the port number, click the message **Plugin configuration needs to be regenerated**.
6. Click **Generate**. When a blank page is displayed, click **Save**.
7. Click **Exit**. Do not just close the browser.
8. Run the server command ENDSBS QEJBAES4
9. Run the server command WRKACTJOB SBS(QEJBAES4)
10. When the subsystem ends, run the server command
STRSBS QEJBAES4/QEJBAES4

If you are using an administrative server other than the default, you should start your administrative server when the subsystem is ready.

11. To start the HTTP server, run one of the following server commands:
 - For an Original HTTP server, run
STRTCPSVR SERVER(*HTTP) HTTPSVR(<http_server_name> '-nolastmod')
 - For an HTTP server powered by Apache, run
STRTCPSVR SERVER(*HTTP) HTTPSVR(<http_server_name>)

SSL port for ASF Tomcat

ASF Tomcat requires no additional configuration steps. To start the HTTP server, run the server command

```
STRTCPSVR SERVER(*HTTP) HTTPSVR(<http_server_name>)
```

Part 3. Using iSeries Access for Web

Chapter 5. Using iSeries Access for Web	41	About	67
Introduction	41		
Logon	41		
Logoff	41		
Bookmark	41		
Realm	41		
URL	41		
Browser Plug-ins	41		
Print	42		
Printer output	42		
Printers	44		
Internet printers	45		
Printer shares	46		
Output queue	46		
Messages	46		
Display messages	47		
Send message	48		
Operator messages	49		
Message queues	49		
5250	49		
Database	49		
Tables	50		
My requests	51		
Run SQL	51		
Copy data to table	54		
Import Request	58		
Database connections	58		
Files	58		
Left Frame	59		
Right Frame	59		
Action Column	59		
Browse files	60		
File shares	60		
Jobs	61		
Jobs	61		
Server Jobs	62		
Command	62		
Search commands	62		
Command prompt	62		
Parameter help	63		
Adding additional values	63		
Run command	63		
Previously run commands	64		
Saved commands	64		
Mail	64		
My Folder	65		
Customize	65		
Preferences	65		
User Profiles	65		
Group Profiles	66		
Selected Profile	66		
Other	66		
Change Password	66		
Connection Pool	66		
Connection Pool Status	67		
Trace	67		

Chapter 5. Using iSeries Access for Web

Introduction

iSeries Access for Web presents a common default look and feel for most of its functions. The default interface contains a header that lists the user profile being used and the iSeries server name. You can navigate through iSeries Access for Web using the list of folders on the left. Click on a folder tab to get a list of the tasks available for that function. Click on a task in the open folder to display that task in the content pane on the right.

Logon

The browser displays a dialog the first time iSeries Access for Web is used in a new browser session. Use a valid iSeries user profile and password to logon.

Each web browser instance tracks the user it is working with. Some browsers, Microsoft Internet Explorer for example, allow you to start more than one instance. Password prompting occurs with each instance, allowing two or more different users to log on using multiple browser instances. You may also use two different browsers at the same time, Microsoft Internet Explorer and Netscape Navigator for example, to log on as different users.

Logoff

iSeries Access for Web uses HTTP Basic authentication for browser authentication and web browsers do not have a "logoff" function, you may need to shut down all browser windows for some browsers in order to log off.

Bookmark

Pages of iSeries Access for Web may be bookmarked for easier access. In wizards, only the first page may be bookmarked.

Realm

The term Realm is used by some browsers when prompting for user name and password. For iSeries Access for Web, a realm is equivalent to the iSeries server name that you are accessing.

URL

Use `http://<server_name>/webaccess/iWAMain` to access the iSeries Access for Web main page. Use `http://<server_name>/webaccess/iWAHome` to access the user customizable home page. Refer to the section on home page customization for more information.

Browser Plug-ins

Some of the data types used by iSeries Access for Web may require either a browser plug-in or application to view the content.

Print

iSeries Access for Web allows you to access printers, output queues, spooled files, printer shares and Internet printers from the iSeries. Print functionality is accessed through the **Print** tab on the iSeries Access for Web navigation bar. An overview of the tasks you can perform using these functions is shown in the content pane.

Any or all of these options can be restricted by customizing the Print function. See "Print" on page 78 for more information.

For a list of restrictions associated with the Print function, see "Print" on page 69.

The Print tab contains the following main options:

- Printer output
- Printers
- Internet printers
- Printer shares
- Output queues

Printer output

Select the Printer output link to see a list of the spooled files which belong to the signed on user. Depending on the customization settings, the list of spooled files that belong to the signed-on user may contain the following information for each spooled file:

File name

The file name that was specified by the user program when the file was created, or the name of the device file used to create this file.

User data

The user-specified data which describe this file.

Creation date and time

The date and time when the file was created.

Pages per copy

The total number of pages or records in the file (pages for print, records for diskette).

Copies

The number of copies remaining to print for files to be processed by a printer writer.

Status The current status of the spooled file. If the status is MSGW (Message Waiting), a link will allow you to display and reply to the message.

Action

The actions below can be performed on the spooled file. The actions displayed are dependent on the status of the spooled file. Supported actions are:

- Hold
- Release
- Print Next
- Delete
- PDF

PDF Transformation Considerations

iSeries Access for Web has two PDF transformation possibilities, IBM Infoprint Server (5722-IP1) or a TIFF transform. IBM Infoprint

Server is a separately purchasable product that gives iSeries Access for Web users the ability to create full text PDF files that deliver document fidelity, while preserving the ability to navigate through the document. If you have IBM Infoprint Server installed, iSeries Access for Web automatically detects and uses it. If you do not have IBM Infoprint Server installed, the individual pages of the spooled file will be converted into images. These images become the pages of the output PDF document. You cannot edit or search for content in any of these pages.

Notes:

1. IBM Infoprint Server may make changes to the order of the spooled files in the current user's list. It may also make changes to the creation date and time and the start and complete date and time.
2. The spooled file must be in either the HELD, READY, or SAVED state to be printed by IBM Infoprint Server.

PDF Output Options

When you select PDF as the printer output action, you may specify configuration settings for the following output options:

- PDF device type
- Drawer 1 paper size
- Drawer 2 paper size
- Destination
 - Browser

You can send the PDF to your browser.

- Mail

You can e-mail the PDF as an attachment to anyone with an e-mail address. For more information on configuring a user profile to use Mail, see "Mail" on page 64.

- Folder

You can save the PDF to your personal folder or the folder of another user.

- Restore original printer output

Preview

The spooled file's contents may be previewed in the following formats:

- GIF
- TIFF
- PCL
- AFPTM Viewer

The TIFF, PCL, and AFP Viewer options require either an additional plug-in or application to perform the viewing.

There are two ways to view AFP output with iSeries Access for Web:

Using AFP Viewer Application

To use the AFP viewer application shipped with iSeries Access for Windows (5277-XE1) to view AFP and SCS output, you will need to associate the application with the AFP and SCS MIME types.

The association of MIME type to application is browser dependent. To associate AFP output with the viewer application, associate the MIME type application/vnd.ibm.modcap or file extension of .afp with the application ftdwinvw.exe, usually found in c:\Program Files\IBM\Client Access\AFPViewr. To associate SCS output with

the viewer application, use the MIME type of application/x-vnd.ibm.SCS or file extension of .scs. Refer to the browser documentation for the details of associating an application to a MIME type.

Using AFP Viewer plug-in

An AFP viewer plug-in that works with Microsoft Internet Explorer and Netscape Navigator can be downloaded from <http://www.printers.ibm.com/R5PSC.NSF/web/afpw>. The plug-in only works for AFP output and is only available as a technology demonstration.

User The name of the user who owns the spooled file.

Job name

The name of the job that produced the spooled file.

Job number

The number of the job that produced this spooled file.

File number

The file number for this spooled file.

Output queue

The name of the output queue that contains the spooled file.

Priority

The output priority assigned to the file. The values range from 1 (highest) to 9 (lowest).

Form type

The type of the forms which should be loaded on the printer.

Printer

The name of the printer specified for this file.

Printers

Select the Printers link to see a list of all printers defined on the system. You can customize your printer view to be either a Basic or an Advanced view. The Basic view allows for high level control of printer function, while the Advanced view allows the individual control of printers, writers, and output queues. The Basic view may contain the following information:

Printer

The name of the printer.

Printer Status

The status of the printer device.

Printer Action

The actions that can be performed to control printer function. The actions displayed are dependent on the status of the printer and its associated resources. The following actions are supported:

- Make available
- Make unavailable
- Start
- Stop
- Hold
- Release

Printer Description

The text describing the printer.

Output Queue

The output queue "attached" to the printer.

Output Queue Status

The status of the output queue.

Writer The name of the writer that is started to the printer.**Current File**

The name of the file that the writer is printing.

Current User

The name of the user that created the file that is currently printing.

Current File User Data

The user-specified data that describes the file being printed.

Current File Form Type

The form type being used by the file being printed.

In addition to the Basic view information items above, the Advanced view may contain the following information:

Printer Action

The actions that can be performed to control the printer device. The actions displayed are dependent on the status of the printer. The printer action column supports the following actions:

- Vary on
- Vary off

Output Queue Action

The actions that can be performed to control the output queue. The actions are:

- Hold
- Release

Writer Status

The status of the writer that is associated with this printer.

Writer Action

The actions that can be performed to control the writer. The actions displayed are dependent on the current status of the writer. The writer action column supports the following actions:

- Start
- Stop
- Hold
- Release
- Change

Internet printers

Select the Internet printers link to see a list of the Internet printers configured on the system. The list of Internet printers includes the following attributes:

Internet printer

The name of the Internet printer. If the Internet printer is a defined printer device, you may click on the linked name to list and work with the printer.

Output queue

The output queue associated with the Internet printer. You may select the linked name of an output queue to see a list of all spooled files that reside on that output queue.

URL The URL used to access the Internet printer.

Printer data type

The type of data expected by the Internet printer.

Printer file

The printer file associated with the Internet printer.

Authentication method

The authentication method used for the Internet printer.

Printer shares

Select the Printer shares link to see a list of the shared printers configured on the system. The list of printer shares includes the following attributes:

Share The name of the printer share. If the share is a defined printer device, you may click on the linked name to list and work with the printer.

Output queue

The output queue associated with the printer being shared. You may select the linked name of an output queue to see a list of the spooled files that reside on that output queue.

Printer driver

The name of the printer driver that clients should use for this print share.

Spooled file data type

The type of the spooled files created for this printer share.

Users The number of users currently accessing the share.

Share description

The text describing the printer share.

Output queue

Select the Output queues link to see a list of all the output queues configured on the system. The list of output queues include the following attributes:

Output queue

The name of the output queue is a link to take the user to a list of the spooled files on the output queue.

Status The status of the output queue.

Action

The actions that can be performed to control the output queue. The actions are:

- Hold
- Release

Files The number of spooled files on the output queue.

Writer The name of the spooling writer that has been started to this output queue.

Messages

iSeries Access for Web allows you to access your message queues on the iSeries. Messages functions are accessed through the **Messages** tab on the iSeries Access for Web navigation bar. An overview of the tasks you can perform using these functions is shown in the content pane.

Any or all of these options can be restricted by customizing the Messages function. See “Messages” on page 81 for more information.

For a list of restrictions associated with the Messages function, see “Messages” on page 69.

The Messages tab contains the following options:

- Display messages
- Send message
- Operator messages
- Message queues

Display messages

Display messages presents a list of the messages in your message queue.

The message list is displayed in a table that has the following columns:

Message ID

Contains an optional message ID which may have a link that, when selected, displays the expanded text and the following information:

- Message text
- Message ID
- Message type
- Severity ranking
- Date message was received
- Time message was received
- Response text field (generated only for Inquiry type messages)

Message text

Contains the actual text of the message as it was sent. The text of the message is automatically wrapped to reduce your need to scroll.

Type Contains the type of the message (Completion, Inquiry and Information) and may have a link that, when selected, displays the following information:

- Message text
- Message ID
- Message type
- Severity ranking
- Date message was received
- Time message was received
- Response text field (generated only for Inquiry type messages)

Date/Time

Displays the date and time that the message was received.

Severity

Displays a numerical value indicating the severity of the message.

Action

Contains a hyperlink that allows you to delete a message from the message queue. Selecting the link deletes the message and updates the message listing.

Remove all messages/Remove all answered messages

Options to Remove All Messages and Remove All Answered Messages are displayed at the bottom of each page of the message listing. Before deleting any messages in your message queue, iSeries Access for Web will display a Confirm remove request prompt.

Click Remove All Messages to permanently delete all of the messages in the message queue.

Click Remove All Answered Messages to permanently delete all the answered messages in the message queue. Messages that require a response will not be removed.

Send message

Send message displays a message form that you can fill out to send a message to another user or queue.

The following are the fields available in the message form:

To users

To send another user a message, type that person's user profile in the To users text box. More than one user may be specified in this text field by using a comma delimited list. At least one user profile must be specified in the To users field or one message queue name must be specified in the To message queues field to send a message.

An Add button is provided that, when clicked, will display a list of the user profiles on the system. You may select one or more of the user profiles in the list. Click OK to add the selected user to the To users field. You may click Cancel to return to the message form without adding any user profiles.

To message queues

The To message queues field is a text box where you can type the name of the message queue that you want to send a message to. At least one user profile or message queue name must be specified to send a message.

Click Add to display a list of the message queues available on the system as well as their descriptions. You may select one or more message queues in the list. Click OK to add them to the To message queues field. You may click Cancel to return to the message form without adding any message queues.

From The From field on the form cannot be specified. Its value is your message queue name.

Message type

You can choose to send an Inquiry or Informational message by clicking the corresponding radio button. Inquiry messages are typically questions, therefore the inquiry type message provides the recipient with the facility to reply to the message.

Informational messages are used as a communication method between users. An informational message requires no response from the recipient.

Message

Type your message into the Message field. The Message field cannot send an empty message. Line feeds and carriage returns are ignored. If they are entered in the Message field, they are discarded before the message is sent.

Click the Send button to submit the message and send it to the specified users and message queues. If the message is sent successfully, you will receive a send confirmation message where you can choose to send another message.

Operator messages

Operator messages displays a list of the messages in the system operator message queue (QSYS/QSYSOPR).

Message queues

Message queues displays a list of the message queues on the system.

The columns in the Message queues listing table are:

Queue

Displays the queue name and, depending on policies, the name may be a link to display all of the messages in that queue.

Description

Displays a description of the message queue.

Action

The Action column, depending on preferences may display a Delete link that will delete the specified message queue. Before completing the delete operation, iSeries Access for Web will ask you to confirm your request.

Create Message Queue option

A Create Message Queue option is displayed at the bottom of each page of the message queue listing. When followed, this link takes the user to a create message queue (CRTMSGQ) prompt. To create a new message queue, fill in the fields as desired, and run the command to create the message queue. After running the command, you will be returned to the Message queues list.

5250

iSeries Access for Web provides an iSeries 5250 user interface. To begin using the 5250 interface, do the following:

1. Open your browser to the iSeries Access for Web main page
http://server_name/webaccess/iWAMain
2. Select the **5250 tab** in the navigation bar.
3. Click **Start Session**.

Access to the 5250 user interface can be restricted. See “5250” on page 84 for more information.

For the latest information on the iSeries Access for Web 5250 user interface, see <http://www.ibm.com/eserver/iseries/access/web/readme.htm>

Database

iSeries Access for Web provides support for accessing database tables on an iSeries server. Database functions are accessed through the **Database** tab on the iSeries Access for Web navigation bar. An overview of the tasks you can perform using these functions is shown in the iSeries Access for Web content pane.

Any or all of these options can be restricted by customizing the Database function. See “Database” on page 85 for more information.

For a list of restrictions associated with the Database function, see “Database” on page 69.

iSeries Access for Web supports defining multiple database connections to access different servers and to use different driver properties. See “Database connections” on page 58 for more information.

The **Database** tab contains the following options:

- Tables
- My requests
- Run SQL
- Copy data to table
- Import request

Tables

The tables list presents a list of the relational database tables on the server. Each table in the list contains links to actions that can be performed on the table. These actions do not require knowledge of SQL and its syntax, but they are not as full-functioned and flexible as the support provided by Run SQL.

The Tables function supports the following actions:

Insert Use the Insert action to insert records into a database table. A form is displayed for entering column values. Required fields are indicated with an *. Fields with defaults are initialized with their default values. Date and time values must be entered in the format corresponding to the current JDBC driver configuration. Insert also supports entering the following SQL register values for date, time and timestamp fields: CURRENT_DATE, CURRENT_TIME, and CURRENT_TIMESTAMP. See “Database connections” on page 58 for more information on JDBC drivers.

Update

Use the Update action to update and delete existing records in a database file. Initially, a query is performed to retrieve the current records in the table. A smaller list of records can be generated by specifying a value, or filter criteria, for one or more fields. From the Records to Update list, a record can be selected for updating or deleting. Choosing the update option results in a form being displayed for changing column values. The current column values are shown, along with an indicator of which fields must not be left blank. When an update or delete is performed, all records matching the selected record are updated or deleted.

When using the update function, date and time values must be entered in the format corresponding to the current JDBC driver configuration. Update also supports entering the following SQL register values for date, time and timestamp fields: CURRENT_DATE, CURRENT_TIME, and CURRENT_TIMESTAMP. See “Database connections” on page 58 for more information on JDBC drivers.

Quick View

Use Quick View to view the contents of a database table.

Run SQL

The Run SQL link provides a quick path to Run SQL. The table list can be used to locate a table and this link can be used to call Run SQL with the SQL statement initialized to SELECT * from *current table*.

Copy data to table

The Copy data to table link provides a quick path to Copy data to table. The table list can be used to locate a table and this link can be used to call Copy data to table, with the table name initialized to the current table.

My requests

Use My requests to manage saved database requests. Saved requests include requests saved using Run SQL or Copy data to table. Imported Client Access Data Transfer requests, saved in either format, are also included in this list. The My requests function supports the following actions:

- Run
- Edit
- Copy
- Rename
- Delete
- Create shortcut

Working with shortcuts

Database requests can only be accessed by the iSeries user profile used to create them. A shortcut is a way to share a request with other users. The following topics describe how the request actions apply to shortcuts:

Create a shortcut

To create a shortcut, a name and an access value must be specified. The access value identifies who will be able to access the shortcut. The access value can be an existing user profile name on the iSeries server, an existing group profile name, or *PUBLIC.

Run a shortcut

When you run a shortcut, the original request is run. If you modify the original request, the shortcut automatically picks up the modified behavior. This is not true for connection information, since the connection information is stored directly with the shortcut. If you update the connection in the original request, the shortcut will not pick up the new connection. If this is not the desired behavior, the shortcut can be deleted and recreated.

Copy a shortcut

Copying a shortcut makes a copy of the original request. Like other requests, the access value for a copied request is the user profile used to create the copy. Therefore, any modifications to the copy do not affect the users of the shortcut.

Delete a shortcut

The creator of a shortcut can delete the shortcut. If the shortcut access is a single user profile, the user with access to the shortcut can also delete it. Only the shortcut creator can delete a group or *PUBLIC shortcut.

Rename a shortcut

Only shortcuts with a single user profile access can be renamed. The shortcut creator or a user with access to the shortcut can rename the shortcut.

Edit a shortcut

You cannot edit a shortcut.

Create a shortcut to another shortcut

You cannot create a shortcut to another shortcut.

Run SQL

Run SQL provides the ability to run SQL statements and to retrieve the results in one of many popular file formats. Any SQL statement, supported by the JDBC driver, can be run. Run SQL only supports the dotted SQL SCHEMA.TABLE naming convention. For example, MYSCHEMA.MYTABLE is a valid table name.

Requests can also be saved for repeated use. For more information about JDBC drivers, see “Database connections” on page 58.

SQL wizard

Run SQL provides an SQL wizard to help build SQL SELECT statements. The resulting statement is set as the value for the SQL statement on the Run SQL page. If necessary, the statement can be modified before running. The SQL wizard steps you through the following parts of building a SELECT statement:

- Selecting a table.
- Selecting and ordering columns.
- Building conditions on character, numeric, date, time, or timestamp fields.
- Specifying how to sort records.

Supported Output types

Most output types support type-specific settings to provide additional customization of the output results. Run SQL supports the following output types:

- Preview
- Comma Separated Value (.csv)
- Data Interchange Format (.dif)
- Extensible Markup Language (.xml)
- Hypertext Markup Language (.html)
- Lotus® 1-2-3® Version 1 (.wk1)
- Microsoft Excel 3 (.xls)
- Microsoft Excel 4 (.xls)
- Portable Document Format (.pdf)
- Text - Plain (.txt)
- Text - Tab Delimited (.txt)

The supported output types for Microsoft Excel and Lotus 1-2-3 are not the newest types supported by these applications. Since the additional capabilities of the newer types are not likely to be needed for retrieving data from a database, this should not result in a loss of functionality. By supporting the older versions of these file types, compatibility can be retained for the older versions of these applications. A newer version of the application can be used to save the results to a file in a newer format.

Note: The file in the new format will not be compatible with Copy data to table.

XML Output Considerations

The XML output generated by Run SQL is a single document containing both an embedded schema and results from the SQL query. The embedded schema is compliant with the W3C Schema Recommendation dated May 2, 2001. The schema contains meta information for the query results portion of the document. Contained in the schema is data type information, limits on data, and document structure.

Current XML parser implementations do not support validation using the embedded approach. Many parsers, including SAX and DOM implementations, require independent documents for the schema and content to do validation. To achieve schema validation with an XML document produced by Run SQL, the document must be restructured into individual data and schema documents. The root elements must also be

updated to support this new structure. Visit the World Wide Web Consortium's web site at <http://www.w3.org> for additional information on XML Schema.

The query results portion of the XML document contains the data returned from the query in a structured row and column fashion. This data may be easily processed by other applications. If more information about the data contained in this section is required, reference can be made to the document schema.

HTML Output Considerations

When the HTML output type is being used, the results are displayed in the browser. To save the results to a file, the browser save function can be used. Another option is to save the SQL request and to redirect the results to a file when the request is run. With Internet Explorer, right-click the Run link and choose the Save Target As option. With Netscape Communicator, hold down the shift key while clicking the Run link.

If the HTML rows per table value is set, Run SQL will display the results in a paged list, similar to Preview, instead of returning a single HTML page.

PDF Output Considerations

The PDF file format represents your SQL data as it would appear on a page. The amount of data that can fit on a page depends on the page size, the page orientation, and the margin sizes. A very large number of columns can result in an unusable PDF document. In some cases, the Adobe Acrobat Reader plug-in cannot load a file like this into the browser. As an alternative, you can break the request into multiple queries, which return subsets of the columns, or you can choose a different output type.

PDF Font Settings

Using the output settings, you can customize the selection of fonts used for the various parts of the PDF document. You can embed the chosen fonts into the document, rather than installing them on the computer used to view the document. Embedding fonts in the document increases the document size.

The character encoding used to represent text is also a PDF output option. If the font is not able to represent a character in the encoding, the character is left blank or another indicator character is used to show the character cannot be displayed. You should choose font and character set values which are capable of representing all characters in the data to display.

By default, Run SQL supports the standard PDF fonts and the Adobe Asian fonts for building PDF output. Since the standard fonts are required to be available with any PDF viewer, there is no need to embed them in the PDF document. Adobe provides a set of Asian font packs for displaying text containing Simplified Chinese, Traditional Chinese, Japanese, or Korean characters. Run SQL supports creating documents with these fonts, but it does not support embedding these fonts in the document. If these fonts are used, the appropriate font pack needs to be installed on the computer used to view the document. These font packs can be downloaded from Adobe's web site at www.adobe.com.

Additional fonts can be added to the available fonts list, using the "Additional PDF font directories" Customization setting. The supported font types are:

- Adobe Type 1 fonts (*.afm)

In order for Type 1 fonts to be embedded into a document, the Type 1 font file (*.pfb) needs to be in the same directory as the font metrics file (*.afm). If only the font metrics file is available, the document can be created with the font, but the computer used to view the document needs to have the font installed. Type 1 fonts only support single-byte encodings.

- TrueType fonts (*.ttf) and TrueType font collections (*.ttc)

Embedding TrueType fonts and TrueType font collections is optional. When a TrueType font is embedded, only the portions of the font needed to represent the data are embedded. The list of available character set encodings is retrieved from the font file. In addition to the retrieved encodings, the multilingual "Identity-H" encoding can be used. When this encoding is used, the font is always embedded into the document. You can embed TrueType fonts, which support double-byte character sets, as an alternative to the Adobe Asian fonts. This generates a larger document, but the computer used to view it does not need to have the font installed.

Run SQL supports building PDF documents with bi-directional data, if the locale of the current request is Hebrew or Arabic.

Output Destinations

The output generated from the SQL request is sent to one of the following destinations:

- **Browser.** The output is either displayed in the browser or a dialog is displayed allowing the results to be opened with an application or saved to disk. The browser page is not updated until the SQL request completes. If the SQL request requires a long time to complete, you may want to choose Mail as attachment or Personal folder for the destination. Browser is the only valid destination choice when the SQL output type is Preview or the output type is HTML and the "rows per table" value is set.
- **Mail as an attachment.** The results of the SQL request are sent to one or more e-mail addresses. You can include message text with the results. You can set the mail information as part of the request or a prompt can be displayed when the request is run. The SQL request runs in the background. A status message is mailed to the originator when the request completes. For information on configuring the SMTP server and a user profile to use Mail, see "Mail" on page 64.
- **Personal folder.** The results of the SQL request are placed in the personal folder for one or more users on the iSeries server. You can set the personal folder information as part of the request or a prompt can be displayed when the request is run. The SQL request runs in the background. A status message is placed in the originator's personal folder when the request completes.

Copy data to table

Use Copy data to table to copy data to a relational database table on the iSeries. Data may be copied from your workstation to an existing relational database table or used to create a new table. Copy data to table requests can be saved for repeated use.

Using Copy data to table

Copy data to table provides a form that assists you in copying data from a workstation file to a database table on the iSeries. The fields available on the Copy data to table form are:

File to Copy

Specify or browse for the workstation file to copy and choose the file type.

The following file types are supported:

- Text - Plain (.txt)
- Comma Separated Value (.csv)
- Microsoft Excel 3 (.xls)
- Microsoft Excel 4 (.xls)
- Data Interchange Format (.dif)
- Lotus 1-2-3 Version 1 (.wk1)
- Text - Tab Delimited (.txt)
- Extensible Markup Language (.xml)

Copy data to table requires the workstation file to follow the conventions of the file type you choose. For example, if you choose Microsoft Excel 3, the file must be a valid Microsoft Excel 3 file.

The file to copy must also contain data in a format that can be copied to a relational database table. Relational database tables consist of columns and rows. Each column in a database table has a name, data type, length, and various other attributes. All data in a database column must be of the same type. A single spreadsheet column may have cells containing various data types (for example, numeric data, formulas, and character data). In order to copy a spreadsheet to a database table, each column of the spreadsheet must contain data of the same type.

Use the settings button to specify additional information about how your data is stored in the file. You can indicate whether the file to copy contains column headings. You should select this option if the file to copy contains headings in the first row. All iSeries Access for Web file types, except plain text, support column headings. You can also set the appropriate character set for the data in the workstation file. In most cases the default character set chosen by iSeries Access for Web should work correctly. If the default character set is not correct, be certain to choose one that properly matches the data in the specified file. An incorrectly chosen character set may result in potential loss of characters, incorrect characters, or corrupt data in the database table.

XML Considerations

Copy data to table requires an XML document to be in a concise format. This format may or may not contain an embedded schema element and its supporting elements. In its simplest form, the XML document must be structured as follows:

```
<?xml version="1.0" encoding="utf-8" ?>
<QiwaResultSet version="1.0">
  <RowSet>
    <Row number="1">
      <Column1 name="FNAME">Jane</Column1>
      <Column2 name="BALANCE">100.25</Column2>
    </Row>
    <Row number="2">
      <Column1 name="FNAME">John</Column1>
      <Column2 name="BALANCE">200.00</Column2>
    </Row>
  </RowSet>
</QiwaResultSet>
```

This format consists of the XML directive, followed by the root element QiwaResultSet. If the encoding attribute is not specified in the XML

directive, copy data to table will assume the document is encoded in utf-8. The root element contains a version attribute. The version corresponding to this format of XML is 1.0. The RowSet element is a container for all the rows of data that follow. These rows of data are contained within Row elements. Each Row element must have a unique numeric number attribute. Within each Row element is one or more Column elements. Each column element within a row must be unique. This is accomplished by adding a sequential numeric suffix. For example, Column1, Column2, Column3, ... Columnx, where 'x' is the number of columns in the row. Each column must also have a name attribute. The name corresponds to the column name in the relational table on the server. If this simple format is used, the 'Validate document with its schema' setting must be turned off since the document does not contain a schema.

Although not required, an XML Schema may also be included in the document. Examine an XML document generated by Run SQL to get an idea of how a schema is structured. Also, visit the World Wide Web Consortium's web site at <http://www.w3.org> for additional information on XML schemas.

Note: Read the "Code disclaimer information" on page 132 for important legal information.

Table to Receive Data

Specify the name of the table to which data will be copied. The table name must be in dotted SQL SCHEMA.TABLE notation. For example, MYSCHHEMA.MYTABLE is a valid table name. If a schema is not specified the default schema for the signed on user will be used.

You can choose whether to replace or append data to an existing table. If the specified table does not exist, you may create a new table based on the format of the workstation file.

Customization allows these options to be enabled or disabled on a per user/per group basis.

Connection

Choose the appropriate connection to communicate with the server from the Connection list.

Copy data to table

Click Copy Data to Table to copy data from a workstation file to a relational database table. The server receives the workstation file, along with the name of the table to receive the data. If the table exists, the format of the table will be verified against the format of the file data. If the table does not exist, you may create a new table based on the format of the PC data. If the formats of the file and database table match, the file data will be copied into the table. If the formats do not match an error will result.

Save request

A saved copy data to table request may be run via a bookmarked page or more commonly by choosing the Run action in the My Requests content pane. Once you have run a saved Copy data to table request iSeries Access for Web will require you to manually enter the name of the file to copy to the server. This feature prevents workstation data files from being sent to web servers without the users knowledge. iSeries Access for Web also displays the name of the file to copy on the Copy data to table panel. For example, if a request was saved to copy data from the file c:\temp\test.txt to the table MYSCHHEMA.TEST the following text displays:

Note: To protect the data on your workstation the file name is not automatically specified.
The original file was: **c:\temp\test.txt**

Using a saved Copy Data to table requests

A copy data to table request may be saved and used at a later time.

1. To save a copy data to table request configure the request, including the following:
 - Workstation file to copy
 - File type
 - Character set
 - Table to receive data
 - Action (replace or append the table)
 - Appropriate connection
2. Click the Save Request button to display the Save Request panel.
3. Provide the name and a description for the request. If a request already exists by that name, choose to replace an existing request. Click OK to save the request.
4. If the request saved successfully the following options will display:
 - Create another request
 - Display My Requests for the current user
 - Run the saved request

Creating a New Table

Create a new relational database table if the specified table does not exist. This new table will be created based on the format of the workstation file to be copied.

When creating a new table users will have two options:

- **View or change column definitions before creating the new table.**

This option is the safest choice. It allows you to verify and if necessary, make modifications to the table's column definitions before creating the table. If the file to copy does not contain column headings, the default column headings of F1, F2, F3, ... Fn (where n is the number of columns in the file to copy) may be changed to something more descriptive. The verification panel also allows you to choose more appropriate data types for various fields (VARCHAR instead of CHAR, or FLOAT instead of NUMERIC.) CHAR and NUMERIC columns may also be lengthened to support larger data in the future.

- **Choose not to verify column definitions**

If you choose not to verify column definitions a default table will be created and workstation file data will be copied into the new default table.

If the file does not contain column headings, default column headings of F1, F2, F3, ... Fn (where n is the number of columns in the file to copy) will be used.

The table will also contain minimum lengths to contain the file data and will use default data types. For example, if 10 characters were required to store the data in the first column of the workstation file, column one of the table would be created as data type CHAR with a maximum length of 10 characters.

After the table definition is correct, choose the Create Table button to create the new table and copy the data from the workstation file to this new table.

Copying a Plain Text file to a table

When a plain text file is copied to a database table, a panel is provided that allows you to indicate individual columns of the file. A plain text file does not have delimiters between its columns like, for example, Comma Separated Value - which separates its columns with a comma. iSeries Access for Web solves this problem by

allowing you to indicate individual columns by placing each column on its own line. This technique only works if the columns in the plain text file are fixed width and uniform throughout the file.

Import Request

iSeries Access for Web allows users to import IBM Client Access for Windows 95/NT or Client Access Express Data Transfer request files. Data Transfer From AS/400® request files are converted to settings that can be used by Run SQL. Data Transfer To AS/400 request files are converted to settings that can be used by Copy data to table. The supported transfer request files are as follows:

- IBM Client Access Express Data Transfer From AS/400 .DTF files
- IBM Client Access for Windows 95/NT Data Transfer From AS/400 .TTO files
- IBM Client Access Express Data Transfer To AS/400 .DTT files
- IBM Client Access for Windows 95/NT Data Transfer To AS/400 .TFR files

Using Import request

To import a Data Transfer request into iSeries Access for Web follow these steps:

1. Type in, or browse to, the name of the Data Transfer request file to import.
2. Choose the correct character set for the data contained in the transfer request file. In many cases the default character set will be appropriate. If the default character set is not correct, be certain to choose one that properly matches the data in the transfer request. Choosing an incorrect character set may result in an incorrectly imported request file.
3. Select Import request. After iSeries Access for Web has processed the request file, a list of import considerations are likely to appear. Read through them carefully.
4. Choose whether to continue or to cancel the import. If continue is chosen, the corresponding iSeries Access for Web function will display.
5. Verify and modify the iSeries Access for Web request if necessary. Due to the differences between Client Access Data Transfer and iSeries Access for Web there is a good chance that the resulting import may require modifications to produce the expected results.
6. Save the request for reuse within iSeries Access for Web as needed.

Database connections

The database function of iSeries Access for Web makes JDBC calls to access the database. By default, the IBM Toolbox for Java driver is used to access the server that iSeries Access for Web is running on.

Customization provides support for defining additional database connections. By defining additional connections, the database code can be switched to access a different database server, to use different driver settings, or to use a different JDBC driver. The ability to define new database connections through Customization is limited to users who are allowed to administer policy settings.

Note: iSeries Access for Web only supports using the IBM Toolbox for Java driver. Using a different driver might work, but this is an untested and unsupported environment.

Files

iSeries Access for Web allows you to access your files on the iSeries. File functions are accessed through the **Files** tab on the iSeries Access for Web navigation bar. An overview of the tasks you can perform using these functions is shown in the iSeries Access for Web content pane.

Any or all of these options can be restricted by customizing the Files function. See “Files” on page 88 for more information.

For a list of restrictions associated with the Files function, see “Files” on page 72.

The **Files** tab contains the following options:

- Browse Files
- File Shares

Browse files opens a list of files in a separate browser window. File shares displays a list of configured shares. You can click on a linked share name to open a separate browser window that will display a list of files for that share. You can navigate through the browse files and file share lists through a tree view in the left frame, or by using navigation features provided in the right frame.

Left Frame

You can navigate the file list using the tree view of directories in the left pane. The tree view lists the subdirectories contained in the specified directory. A triangle pointing right, or “+”, indicates that a directory may be expanded to show the subdirectories that it contains. A triangle pointing down, or “-”, indicates the subdirectory may be hidden.

Right Frame

Directory names appear as links that allow you to easily navigate the subdirectories. File names will appear as links that allow the file to be downloaded to the local file system or displayed in a browser window. Navigation back to a higher level directory is provided by a “..” (Parent Directory) link. The “Directory Contents” heading provides a quick navigation feature allowing you to easily navigate to any of the subdirectories displayed in the path. All of the navigation features can be controlled through the policies on the **Customize** tab.

The right frame contains a table with the following:

Name Contains the name of the directory or file.

Size Contains the size of the file in bytes, this column is blank for directories.

Type Indicates whether the name is for a directory or file.

Modified

Contains the date that the directory or file was last modified.

Action

Allows you to rename, copy, delete, or mail a file. Allows you to create, rename, or delete a directory.

Action Column

Using the Action column you can rename, copy, delete, or mail a file in the current directory or subdirectory. You can also create, rename, or delete a directory. If the iSeries NetServer file share is read-only, you will not be able to perform any actions. Using Customize, you can turn this column off, or restrict a user from any of the actions. See “Files” on page 88 for more information.

Create

You can create a new directory. The current directory path will be displayed so you can verify the location of your directory.

Copy

You can copy a file to another file or directory. The current directory path will be displayed so you can verify you selected the correct file to copy.

Rename

You can rename an existing directory or file.. The current name will be displayed so you can verify that you selected the correct file or directory to be renamed.

Delete

You can select a file or directory to delete. The current directory path is displayed so you can verify you selected the correct file or directory to be deleted. Once you have confirmed that you want to delete the file or directory, click on Delete File. This action cannot be undone.

Mail

You can mail a file to an e-mail address. The current directory path will be displayed so you can verify you selected the correct file to send.

Browse files

Lists the directories and files on the server that iSeries Access for Web is running on.

File shares

Lists the iSeries NetServer file shares on the server that iSeries Access for Web is running on. The file shares list consists of a table with the following columns:

Share Name

The Share Name is a link that will display contents of the NetServer file share in a separate browser window. This function can be controlled through the policies on the Customize tab.

Description

The text description of the iSeries file share.

User Count

User Count displays the number of users that are actively connected to this iSeries NetServer file share.

Permission

Displays whether the file share is Read only or Read/Write.

File Content-type (MIME-type) mapping

iSeries Access for Web uses the file extension to determine the file content-type (MIME-type). The file content-type is used by the browser to determine how best to render the information. For example, files with an extension of .htm, .html, or .txt are rendered in the browser window. The browser will also attempt to determine what browser plug-in to use for the given file content-type. A file with a .pdf extension will cause the browser to attempt to load the Adobe Acrobat Reader.

iSeries Access for Web provides a way to extend or override the shipped file extension to file content-type mapping. These overrides are done on an instance basis. For each web application server (WebSphere and ASF Tomcat) instance that iSeries Access for Web is configured for, you can override the shipped file extension content-type mapping.

To override the shipped mappings, create a file called extension.properties and place the file in the integrated file system at /QIBM/UserData/Access/Web2/<application_server>/<instance_name>/config.

Replace <application_server> with:

- was40adv for a WebSphere 4.0 Advanced Edition configuration
- was40sng for a WebSphere 4.0 Advanced Single Server Edition configuration
- asftomcat for a ASF Tomcat configuration

Replace <instance_name> with the name of the web application server instance that was configured using the QIWA2/CFGACCWEB2 command to configure iSeries Access for Web.

Some examples of extension.properties entries:

- out=text/plain
- lwp=application/vnd.lotus-wordpro

For a list of file content-types, see <ftp://ftp.isi.edu/in-notes/iana/assignments/media-types/media-types>.

Jobs

iSeries Access for Web allows you to access jobs on the iSeries through either the user job list or the server job list. Jobs functions are accessed through the **Jobs** tab on the iSeries Access for Web navigation bar. The content pane shows an overview of the tasks you can perform using these functions.

Any or all of these options can be restricted by customizing the Jobs function. See “Jobs” on page 82 for more information.

The Jobs tab contains the following options:

- Jobs
- Server jobs

Jobs

Select the Jobs link to see a list of the user jobs that belong to the signed on user. By default, the user job list will contain active jobs and queued jobs shown with the following attributes:

Job The name of the user job.

Status The current status of the job.

Type The type of user job.

Entered System

The date and time the job entered the system.

Action

The actions that can be performed on the user job. The actions displayed are dependent on the current status of the user job. Supported actions are:

- Hold
- Release
- Delete/End
- Job Log
- Printer Output
- Properties

Use the Job Preferences function to add additional user job attributes to the list.

Server Jobs

Select the Server jobs link to see a list of the server jobs that are running on behalf of the signed on user. By default, the list of server jobs include the following attributes:

Job The name of the server job.

Detailed Status

The current detailed status of the job.

Server The descriptive name of the server job.

Run Priority

The current run priority assigned to the server job.

Thread Count

The current number of threads associated with the server job.

Action

The actions that can be performed on the server job. The actions displayed are dependent on the current status of the server job. Supported actions are:

- Hold
- Release
- Delete/End
- Job Log
- Properties

Use the Job Preferences function to add additional server job attributes to the list.

Command

The **Command** tab contains support for running batch level iSeries commands, searching for CL commands on the iSeries, and running previously saved commands. Interactive commands can be prompted and run, but their usefulness is limited since only success or failure will be shown. If *PRINT is specified for the output, you can run an interactive command and view the spooled file output using the iSeries Access for Web Print function.

For information on customizing the Command function, see “Command” on page 91.

For a list of restrictions associated with the Command function, see “Command” on page 72.

Search commands

You can search for a specific command using the following methods:

- By command name.
- By command text description.

Command prompt

If an incomplete command is specified, the Command function supports prompting the command to help a user complete the command they wish to run.

The command prompt accepts the following:

- A command name.
- A partially completed command line.
- A complete command line.

In the case of a partially completed command line, the command prompting code will take specified parameter values from the command line and show them in the command prompt page.

Parameter help

In addition to the basic prompting function, the command prompter page also displays help for individual parameters of a command. The following icon appears next to parameters that have help available for them:



Select the icon and a new browser window will appear with help for the specified parameter. If the help window is kept open, and help is selected for another parameter of the same command, the "help" window will show help for the newly specified parameter. If help is selected for a different command, a new help window will be opened.

Adding additional values

Parameters allowing more than one value are also supported. Parameters that support more than one value have the following icon by them:



If more values are required, click on the icon and a page will display to allow more values to be entered. From this page you can save the new values entered, or cancel and return to the previous page.

Run command

Select the Run command button or the Submit batch job button to run the command. You can select the following output types for the completion status message:

- **Browser**

You can send the completion status message to your browser.

- **Mail**

You can e-mail the completion status message to your e-mail address.

- **Folder**

You can save the completion status message to your personal folder.

Note: If you send the completion status message as an e-mail attachment or personal folder item, control is returned to your browser window. This allows you to submit additional Run command requests or perform a different function without having to wait for the command to complete.

The command function allows you to run a new command, or to select a previously run command from the previous commands list. You can control the size of this list using the Customization function.

Previously run commands

Commands run previously in the current browser session are displayed in a list on the Run command page. These commands are only accessible from the current browser session, and are not saved for reuse. You may Run, Prompt, Retrieve, or Remove a previously run command.

The Retrieve option will load the command string into the command entry field, allowing minor command modifications to be performed without having to reprompt the entire command.

The Remove option will remove the command from the previously run command's list. The Remove option does not remove the underlying CL command from the server. The Remove option may be desirable if you run a command containing sensitive or confidential information.

Saved commands

A Save link on a previously run command allows you to name and save a command for later use. The user who saved the command can access the saved command from any browser session. You can also overwrite an existing named command with a new command. You must run a command before you save it to ensure the command is valid. Access saved commands through the **My Commands** tab item. The list of saved commands contains the following information about each command:

- Name
- Command
- Output
- Action
- Last access

Mail

iSeries Access for Web allows you to e-mail database query results, printer output PDFs, command completion notifications, and other files to anyone with an e-mail address.

The mail function is available from several places in iSeries Access for Web, including **Database**, **Files**, and **Commands**. You can also send e-mail notifications to users when items are saved in their personal folders.

To use the Mail function you must first have an e-mail address configured for your user profile. The administrator may configure this, or the administrator may allow users to configure their own e-mail address in the Mail Preferences portion of the **Customize** tab on the iSeries Access for Web navigation bar. The administrator must also specify the name of the SMTP mail server to be used by the user profile or group. You can also use Mail Preferences to restrict users from Mail. For more information on the Preferences portion of the **Customize** tab on the iSeries Access for Web navigation bar, see Chapter 8, "Preferences" on page 99.

For information on customizing the Mail function, see "Mail" on page 92.

My Folder

My Folder contains a list of the items that have been put in the current user's personal folder, either by the current user or another user. The list may contain the following information about the items:

- Item description
- Status
- From
- Date/Time
- Size

My Folder also includes an Actions column which lists the actions available for the items in the folder. The list may contain the following actions:

- Open the item
- Rename the item
- Delete the item
- Mark the item as Opened or Unopened
- Send the item to an e-mail address

iSeries Access for Web allows you to edit the My Folder list in the following ways:

- Mark all opened
- Mark all unopened
- Delete all opened items
- Delete all items
- Delete selected items

Customize

iSeries Access for Web allows you to set preferences to control how information is presented to you while using iSeries Access for Web. Administrators are able to customize settings for other users or groups to control which functions are available. Since an iSeries user profile is required to access iSeries Access for Web, customized settings are associated with user profiles. Customized settings can also be associated with iSeries group profiles, so members of groups without settings specific to their user profile will inherit settings from their group profiles. This allows administrators to easily customize the settings for whole groups of users without having to customize all users individually.

Preferences

The Preferences function on the **Customize** tab allows users to control how information is presented to them. By default, users are able to set their own preferences. Any preference modifications will be saved and associated with their iSeries user profile.

See Chapter 8, "Preferences" on page 99 for more information on this function.

User Profiles

The User Profiles function on the **Customize** tab is available only to iSeries Access for Web administrators. This function displays a list of user profile names retrieved from the iSeries server. The list of profiles includes the ones the administrator is allowed to update. From this list, the administrator can select a user profile to customize. See Chapter 9, "Administering Users and Groups" on page 101 for more information on how to administer iSeries Access for Web policy settings.

Group Profiles

The Group Profiles function on the **Customize** tab is available only to iSeries Access for Web administrators. This function displays a list of group profile names retrieved from the iSeries server. The list of profiles includes the ones the administrator is allowed to update. From this list, the administrator can select a group profile to customize. A special group profile, *PUBLIC, can be used to customize default settings for all users. See Chapter 9, “Administering Users and Groups” on page 101 for more information on how to administer iSeries Access for Web policy settings.

Selected Profile

The Selected Profile function on the **Customize** tab is available only to iSeries Access for Web administrators. This function allows administrators to customize profiles by entering a specific user or group name. See Chapter 9, “Administering Users and Groups” on page 101 for more information on this function.

Other

iSeries Access for Web provides access to other tasks which can be performed on your iSeries server.

Any or all of these options can be restricted by customizing the Other function, see “Other” on page 96 for more information.

Change Password

iSeries Access for Web allows the logged on user to change their password.

Note: iSeries Access for Web uses HTTP Basic Authentication to authenticate each request. When the password is changed, the subsequent request will fail authentication and the browser will prompt for the user name and new password.

Connection Pool

iSeries Access for Web makes use of the iSeries Access servers to perform many of its tasks. Connections to these servers can be managed based on the following criteria:

Connection Pool Settings	Description
Cleanup interval	Specifies how often to check the pool of connections and close any connections that do not meet the other criteria.
Connections per user	Specifies the maximum number of active connections per user. Attempts to open additional connections will wait until a connection becomes available.
Maximum inactivity	Specifies the amount of time an idle connection will be available before it is closed.
Maximum lifetime	Specifies the amount of time a connection will exist before it is closed.
Maximum use count	Specifies the number of times a connection can be used before it is closed.
Maximum use time	Specifies the amount of time a connection can be active before it is closed.

Connection Pool Status

iSeries Access for Web provides summary and per user status of connections to the iSeries Access servers. The following information is provided:

Table 10. Connection Summary

Connection Pool Status	Description
Active connections	The number of connections that are in use performing a task, such as executing a command or retrieving data.
Available connections	The number of connections that are idle.
Total connections	The total number of connections. This is the sum of active and available connections.
Total users	The total number of users that have had connections since iSeries Access for Web was started. This number includes users that no longer have any connections.
Active users	The total number of users that have active or available connections.

Table 11. Connection Details

Column	Description
System	The currently connected system.
User	The currently connected user.
Active	The total number of active connections.
Available	The total number of active connections.
Action	Contains a Clear link that will clear all connections from the connection pool for that system/user.

Trace

iSeries Access for Web provides tracing capabilities for problem determination. If reporting a problem, IBM Service will provide information on using these capabilities.

About

iSeries Access for Web provides information about itself and its environment.

Chapter 6. Restrictions

Print

Previewing any spooled file using the GIF and TIFF preview options

Multiple PTFs are required to display documents containing more than one page.
The PTFs are:

- SI02028
- SI02756

Previewing AFP data

AFP data may not view properly when previewing with the GIF, TIFF and PCL preview functions. If the data was created using one of the IBM AFP printer drivers and the "Print Text as Graphics" option in the document defaults settings of the driver is turned "Off", then the "Fonts" device setting must be set to an EBCDIC code page.

Previewing spooled files using the AFP Viewer preview option

The external resources in AFP spooled files will not be displayed.

Unknown File Type Error Message when attempting to Preview using Netscape

If attempting to preview in AFP format, select "Pick App" and then, for example, "C:\Program Files\IBM\Client Access\AFPVIEWR\ftdwinvw.exe". You may also install the AFP Viewer plug-in located at <http://www.printers.ibm.com/R5PSC.NSF/web/afpwb>. The plug-in only works for AFP output and is only available as a technology demonstration.

If attempting to preview in PCL or TIFF format, you will need to purchase a PCL or TIFF viewer and install it.

Messages

A list of Send message restrictions and possible problems follows:

- When sending messages to message queues, the target message queue can only reside in a library where the library name is 9 characters or less.
- Break messages are not supported. Break messages can be sent using the Command function.

Database

A list of Database restrictions and possible problems follows:

- iSeries Access for Web only supports using the IBM Toolbox for Java JDBC driver, to access the database server. Although other drivers might work, this is an unsupported and untested environment.
- The iSeries Access for Web preferred language setting is not used on database connections. Therefore, all messages received from the database server will be in the language derived from the LANGID and CNTRYID of the user profile used to start the WebSphere Application Server.

Tables

The table list returns relational database tables, aliases, and views. Non-relational database tables are not returned.

Insert

A list of Insert restrictions and possible problems follows:

- Insert does not support binary large object (BLOB) and integer with scale column types. Insert does support the character large object (CLOB) column type, however, entering a very large value could potentially consume all of the browser's memory. All other column types, supported by the iSeries, are supported by Insert.
- Insert only supports setting the URL portion of a datalink.
- Insert does not provide a way to insert null column values, unless the default value for a field is null and the field value is left unchanged.

Update

A list of Update restrictions and possible problems follows:

- Update does not support binary large object (BLOB) and integer with scale column types. Update does support the character large object (CLOB) column type, however, entering a very large value could potentially consume all of the browser's memory. All other column types, supported by the iSeries, are supported by Update.
- Update only supports setting the URL portion of a datalink.
- Update does not provide a way to set null column values. However, if a column has a null value and the field is left blank, the column value will remain null.

Shortcuts

Connection information is stored directly with a shortcut. Therefore, when the connection in the original request is changed, the shortcut does not pick up the new connection.

Run SQL

A list of Run SQL restrictions and possible problems follows:

- You can not run a saved MS Excel 3 or MS Excel 4 request from a Netscape browser, if you have the NCompass DocActive plug-in installed. You can run these requests dynamically, using the Run SQL button.
- On Windows 2000 using Internet Explorer, if you have Microsoft Excel installed and you try to output your results to MS Excel 3 or MS Excel 4, you will be prompted to logon to the iSeries server again. This will cause an additional license to be used. This only happens the first time you try to load an Excel file into the browser. As an alternative, you could save the request without running it, run the saved request, and redirect the results to a file. This is done by right-clicking on the Run link and choosing the Save Target As option. After saving the SQL output file, you could load it using Microsoft Excel or some other application.
- If you choose PDF as the output type and the SQL statement generates a very large number of columns, the resulting output might be too compressed to read, or might be a blank page. In this case, use a different page size, choose a different output type, or modify the SQL statement to return a subset of the columns.
- If you are using the Opera browser and your output contains very long column data, your data may be truncated when displayed.

- Run SQL supports retrieving tables with character large object (CLOB) column types with the following restrictions:
 - Output types with a maximum cell size, such as Microsoft Excel and Lotus 1-2-3 version 1, will truncate the data if it exceeds the maximum cell size.
 - Other output types will not truncate the data, however, retrieving very large values could potentially consume all of the browser's memory.
- If you use Microsoft Internet Explorer, choose PDF as the output type, and get a blank page instead of the SQL output, try one of the following circumventions:
 - Ensure you have the installed the latest version of Microsoft Internet Explorer.
 - Instead of running the request directly from Run SQL, save the request and use the Run action from My Requests.
 - Change your Adobe Acrobat Reader configuration to display the reader in a separate window, instead of within the browser.

SQL wizard

A list of SQL wizard restrictions and possible problems follows:

- Only single table selects are supported.
- Nested conditions are not supported.
- Building conditions is supported for the column types supported by the iSeries, with the following exceptions: Binary large objects (BLOBS), Character large objects (CLOBs), and Datalinks.

Copy data to table

To copy an XML document to the server, the document must be the same XML format as generated by Run SQL. An embedded schema is required only if the document is set to **Validate document with its schema**. See 55 for details.

Import request

Several potential problems and restrictions exist when importing a Client Access or Client Access Express Data Transfer request into iSeries Access for Web. If any problems or restrictions are detected, a warning will be displayed on an import considerations panel. A list of these potential problems and restrictions follows:

- Importing a request containing a reference to a file member will result in the member being removed from the file name. iSeries Access for Web will only provide access to the default member of a file (table).
- Certain Data Transfer From AS/400 statements can not be converted into statements that can be modified by the SQL Wizard. The SQL Wizard does not support building or editing SQL statements containing GROUP BY, HAVING or JOIN BY clauses. In this case, you must hand-edit the resulting statement on the Run SQL panel.
- Data Transfer has an option for specifying whether ANSI or ASCII data is written to or read from a PC file. Requests imported into iSeries Access for Web will use the Data Transfer setting, combined with the language and character set specified by the browser to determine the encoding of the client file. This may or may not be correct. You may have to manually change this setting.
- iSeries Access for Web will not differentiate between source physical and data physical files. An imported request that selects all columns (SELECT *) from a source physical file will produce output containing all columns contained within the source physical file, including the sequence and date columns. An identical request run with Client Access Express produces output containing only the data column(s).
- When importing Client Access Data Transfer to AS/400 requests that copy data to a source physical file, the request must be using an FDF file. This situation

cannot be detected by the import function and an error will not be issued. However, if an FDF was not being used, the resulting copy data to table request will not work correctly.

- iSeries Access for Web does not support all the file types currently supported by Client Access Data Transfer. In some cases, a Data Transfer file type may be mapped to a corresponding iSeries Access for Web file type. If a corresponding file format cannot be found the import will fail.
 - Some output options available in Client Access Data Transfer are not available in iSeries Access for Web. These options will be ignored.
-

Files

A list of File restrictions and possible problems follows:

- There is currently a 2147483647 byte (approximately 2 GB) limit maximum for files that are created on the server during the Copy File function. This limitation is a result of the O_LARGEFILE flag not being supported by the iSeries Optimized File Server.
 - Some browser implementations limit the overall size of the URL that can be used, this will result in an indirect limit on the size of the fully qualified file name (combination of the path and the file name) that can be used with the Browse files and Browse shares functions. For example, there is approximately a 2K limit on the URL for Microsoft Internet Explorer and approximately a 4K limit in Opera and Netscape.
-

Command

A list of Command prompting restrictions follows:

- Prompt controls and Prompt control programs for parameters are not supported.
 - Key parameters/prompt override programs are not supported.
 - Parameter value validity checking is not performed.
 - "Command mapping" exit programs are not supported.
 - Selective prompting characters are not supported.
-

Web Browsers

A list of web browser restrictions and possible problems follows:

- If you experience problems logging on, or completing authentication, when first using iSeries Access for Web, ensure that the user profile and password you supply contain combinations of the following characters. Using characters other than the following below can cause the logon/authentication to fail:
 - A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
 - 0 1 2 3 4 5 6 7 8 9
 - _ (the underscore)
 - iSeries Access for Web requires that the web browser allow cookies. For information about how to set your browser's cookie configuration, see "Web Browser Requirements" on page 14.
-

Opera

A list of Opera restrictions and possible problems follows:

- Opera V5.02 only supports passwords up to 99 characters in length.
- When using the Opera browser, the Back link on many pages (not the Back button) may not work correctly.
- The Opera 6.0 browser cannot display PDF documents using the Adobe Acrobat Reader plug-in if the URL used to access the document contains parameters.

Part 4. Administering and Customizing iSeries Access for Web

Chapter 7. iSeries Access for Web Policies	75
Introduction	75
General.	75
Print.	78
Messages	81
Jobs	82
5250.	84
Database	85
Files.	88
Command.	91
Mail.	92
My Folder.	93
Administration	94
Other	96
Chapter 8. Preferences	99
Introduction	99
Categories of Preferences	99
Use Preferences	99
Restrict Access to Preferences	100
Chapter 9. Administering Users and Groups	101
Introduction.	101
Who Can Administer Other Users and Groups	101
Determine Policy Settings for a User	101
Customize User Profiles.	102
Deny Access to Functions	103
Customize Group Profiles	103
*PUBLIC Group Settings	103
Copying Policy Settings to Other Profiles	103
Strategies for Customizing iSeries Access for Web	104
Chapter 10. Customize the Home Page and Template File	105

Chapter 7. iSeries Access for Web Policies

Introduction

iSeries Access for Web provides application level control to functions via a collection of policy settings that can be administered at the iSeries user and group profile level. This chapter contains descriptions for all of the policy settings. Some of these settings are also referred to as preferences. Preferences are settings that users can modify to tailor the iSeries Access for Web application to meet their needs. For more information on preferences and administering users and groups, refer to Chapter 8, "Preferences" on page 99 and Chapter 9, "Administering Users and Groups" on page 101.

General

These policies control the layout and language of iSeries Access for Web pages.

Table 12. General Policies

Policy	Description	Values	Default Value	Pref-erence
Home page HTML file	Specifies the HTML file to display when the iWAHome URL is invoked. This page is referred to as the iSeries Access for Web home page. See Chapter 10, "Customize the Home Page and Template File" on page 105 for more details.	A fully qualified iSeries integrated file system path.	/QIBM/ProdData/Access/Web2/html/homepage.html	No
Template HTML file	Specifies the HTML file to use as a template when any iSeries Access for Web URL is invoked. See Chapter 10, "Customize the Home Page and Template File" on page 105 for more details.	A fully qualified iSeries integrated file system path.	/QIBM/ProdData/Access/ Web2/html/ webaccess.html	No
Navigation bar	Controls whether the navigation bar is visible. The navigation bar contents are controlled by policies that specify whether tabs are visible or functions are restricted.	Show, Hide	Show	No
Default rows per page	Specifies the number of rows of a list that are shown on a page. If the number of rows in the list exceeds this value, additional pages are created.	Any integer greater than 0	25	Yes
Default pages per set	Specifies the number of pages of a list that are directly accessible via the page navigation links. The page navigation links provide direct access to the first page, the previous set of pages, the previous page, the pages in the current set, the next page, the next set of pages, the last page and to refresh the list.	Any integer greater than 0	10	Yes

Table 12. General Policies (continued)

Policy	Description	Values	Default Value	Preference
Preferred language	Specifies the language that you can view pages in. See “Language and Character Set Selection” on page 113 for more details.	See Table 13 on page 77.	None	Yes
Preferred character set	Specifies the character set you prefer to view pages in. See “Language and Character Set Selection” on page 113 for more details.	See Table 14 on page 78.	None	Yes
PDF font directories	Indicates the integrated file system directory (or directories) that are searched for Adobe Type 1, TrueType, or TrueType collection font files used to support PDF output. These directories have either been specified at the *PUBLIC group level, or at a group level for this profile.	Read-only informational setting indicating which directories will be searched based on group membership.	None	No
Additional PDF font directories	Specifies an integrated file system directory (or directories) containing additional Adobe Type 1, TrueType, or TrueType collection font files to be supported for PDF output.	A fully-qualified iSeries integrated file system directory path. Use a semicolon to separate multiple directories.	None	No

Table 13. Supported Languages

Language
<ul style="list-style-type: none"> • Albanian [sq] • Albanian (Albania) [sq-AL] • Arabic [ar] • Arabic United Arab Emirates) [ar-AE] • Arabic (Bahrain) [ar-BH] • Arabic (Algeria) [ar-DZ] • Arabic (Egypt) [ar-EG] • Arabic (Iraq) [ar-IQ] • Arabic (Jordan) [ar-JO] • Arabic (Kuwait) [ar-KW] • Arabic (Lebanon) [ar-LB] • Arabic (Libya) [ar-LY] • Arabic (Morocco) [ar-MA] • Arabic (Oman) [ar-OM] • Arabic (Qatar) [ar-QA] • Arabic (Saudi Arabia) [ar-SA] • Arabic (Sudan) [ar-SD] • Arabic (Syria) [ar-SY] • Arabic (Tunisia) [ar-TN] • Arabic (Yemen) [ar-YE] • Bulgarian [bg] • Bulgarian (Bulgaria) [bg-BG] • Byelorussian [be] • Byelorussian (Belarus) [be-BY] • Catalan [ca] • Catalan (Spain) [ca-ES] • Chinese [zh] • Chinese (China) [zh-CN] • Chinese (Hong Kong S.A.R.) [zh-HK] • Chinese (Singapore) [zh-SG] • Chinese (Taiwan) [zh-TW] • Croatian [hr] • Croatian (Croatia) [hr-HR] • Czech [cs] • Czech (Czech Republic) [cs-CZ] • Danish [da] • Danish (Denmark) [da-DK] • Dutch [nl] • Dutch (Belgium) [nl-BE] • Dutch (Belgium,Euro) [nl-BE-EURO] • Dutch (Netherlands) [nl-NL] • Dutch (Netherlands,Euro) [nl-NL-EURO] • English [en] • English (Australia) [en-AU] • English (Belgium) [en-BE] • English (Canada) [en-CA] • English (China) [en-CN] • English (United Kingdom) [en-GB] • English (Ireland) [en-IE] • English (Ireland,Euro) [en-IE-EURO] <ul style="list-style-type: none"> • English (Japan) [en-JP] • English (South Korea) [en-KR] • English (New Zealand) [en-NZ] • English (Singapore) [en-SG] • English (Taiwan) [en-TW] • English (United States) [en-US] • English (South Africa) [en-ZA] • Estonian [et] • Estonian (Estonia) [et-EE] • Finnish [fi] • Finnish (Finland) [fi-FI] • Finnish (Finland,Euro) [fi-FI-EURO] • French [fr] • French (Belgium) [fr-BE] • French (Belgium,Euro) [fr-BE-EURO] • French (Canada) [fr-CA] • French (Switzerland) [fr-CH] • French (France) [fr-FR] • French (France,Euro) [fr-FR-EURO] • French (Luxembourg) [fr-LU] • French (Luxembourg,Euro) [fr-LU-EURO] • German [de] • German (Austria) [de-AT] • German (Austria,Euro) [de-AT-EURO] • German (Switzerland) [de-CH] • German (Germany) [de-DE] • German (Germany,Euro) [de-DE-EURO] • German (Luxembourg) [de-LU] • German (Luxembourg,Euro) [de-LU-EURO] • Greek [el] • Greek (Greece) [el-GR] • Hungarian [hu] • Hungarian (Hungary) [hu-HU] • Icelandic [is] • Icelandic (Iceland) [is-IS] • Italian [it] • Italian (Switzerland) [it-CH] • Italian (Italy) [it-IT] • Italian (Italy,Euro) [it-IT-EURO] • Hebrew [iw] • Hebrew (Israel) [iw-IL] • Japanese [ja] • Japanese (Japan) [ja-JP] • Korean [ko] • Korean (South Korea) [ko-KR] • Lithuanian [lt] • Lithuanian (Lithuania) [lt-LT] • Macedonian [mk] • Macedonian (Macedonia) [mk-MK] <ul style="list-style-type: none"> • Norwegian [no] • Norwegian (Norway) [no-NO] • Norwegian (Norway,Bokmål) [no-NO-B] • Norwegian (Norway,Nynorsk) [no-NO-NY] • Polish [pl] • Polish (Poland) [pl-PL] • Portuguese [pt] • Portuguese (Brazil) [pt-BR] • Portuguese (Portugal) [pt-PT] • Portuguese (Portugal,Euro) [pt-PT-EURO] • Romanian [ro] • Romanian (Romania) [ro-RO] • Russian [ru] • Russian (Russia) [ru-RU] • Serbian [sr] • Serbian (Yugoslavia) [sr-YU] • Slovak [sk] • Slovak (Slovakia) [sk-SK] • Slovenian [sl] • Slovenian (Slovenia) [sl-SI] • Spanish [es] • Spanish (Argentina) [es-AR] • Spanish (Bolivia) [es-BO] • Spanish (Chile) [es-CL] • Spanish (Colombia) [es-CO] • Spanish (Costa Rica) [es-CR] • Spanish (Dominican Republic) [es-DO] • Spanish (Ecuador) [es-EC] • Spanish (Spain) [es-ES] • Spanish (Spain,Euro) [es-ES-EURO] • Spanish (Guatemala) [es-GT] • Spanish (Honduras) [es-HN] • Spanish (Mexico) [es-MX] • Spanish (Nicaragua) [es-NI] • Spanish (Panama) [es-PA] • Spanish (Peru) [es-PE] • Spanish (Puerto Rico) [es-PR] • Spanish (Paraguay) [es-PY] • Spanish (El Salvador) [es-SV] • Spanish (Uruguay) [es-UY] • Spanish (Venezuela) [es-VE] • Swedish [sv] • Swedish (Sweden) [sv-SE] • Thai [th] • Thai (Thailand) [th-TH] • Turkish [tr] • Turkish (Turkey) [tr-TR] • Ukrainian [uk] • Ukrainian (Ukraine) [uk-UA]

Table 14. Supported Character Sets

Character Sets	
<ul style="list-style-type: none"> • Western [ISO-8859-1] • Western [windows-1252] • Arabic [windows-1256] • Arabic [ISO-8859-6] • Arabic [ASMO-708] • Baltic [windows-1257] • Baltic [ISO-8859-4] • Central European [ISO-8859-2] • Central European [windows-1250] • Central European [cp852] • Simplified Chinese [GB2312] • Simplified Chinese [EUC-CN] • Traditional Chinese [Big5] • Traditional Chinese [cp950] • Traditional Chinese [EUC-TW] • Cyrillic [windows-1251] • Cyrillic [KOI8-R] 	<ul style="list-style-type: none"> • Cyrillic [ISO-8859-5] • Cyrillic [cp866] • Cyrillic [cp855] • Greek [ISO-8859-7] • Greek [windows-1253] • Hebrew [windows-1255] • Hebrew [ISO-8859-8] • Hebrew [cp862] • Japanese [Shift_JIS] • Japanese [EUC-JP] • Korean [EUC-KR] • Korean [cp949] • Thai [cp874] • Turkish [ISO-8859-9] • Turkish [windows-1254] • Vietnamese [windows-1258] • Multilingual [UTF-8]

Print

The following policies control access to the Print tasks.

Table 15. Print Policies

Policy	Description	Values	Default Values	Preference
Print tab	Controls whether the Print tab is displayed.	Show, Hide	Show	Yes
Printer output	Controls access to the Printer output function, and whether the Printer output item is available on the Print tab in the navigation bar. When set to Allow, users are allowed to list, preview, and manage their spooled printer files.	Allow, Deny	Allow	No
Hold/release printer output	Controls whether Hold and Release actions may be performed on a spooled file.	Allow, Deny	Allow	No
Print next	Controls whether the Print next action may be performed on a spooled file.	Allow, Deny	Allow	No
Delete printer output	Controls whether the Delete action may be performed on a spooled file.	Allow, Deny	Allow	No
PDF Transform	Controls whether the transform to PDF output action can be performed on a spooled file.	Allow, Deny	Allow	No
GIF preview	Controls whether a GIF formatted preview of the spooled file is allowed.	Allow, Deny	Allow	No
TIFF preview	Controls whether a TIFF formatted preview of the spooled file is allowed.	Allow, Deny	Allow	No

Table 15. Print Policies (continued)

Policy	Description	Values	Default Values	Preference
PCL preview	Controls whether a PCL formatted preview of the spooled file is allowed.	Allow, Deny	Allow	No
AFP preview	Controls whether an AFP formatted preview of the spooled file is allowed.	Allow, Deny	Allow	No
Printer output list columns	Specifies the identity and order of the columns to be displayed when viewing printer output.	File Name, User Data, Creation Date/Time, Pages Per Copy, Copies, Status, Action, Preview, User, Job Name, Job Number, File Number, Output Queue, Priority, Form Type, Printer	File Name, User Data, Creation Date/Time, Pages Per Copy, Copies, Status, Action, Preview, User, Job Name, Job Number, File Number, Output Queue, Priority, Form Type, Printer	Yes
Printers	Controls access to the Printer function, and whether the Printers item is available on the Print tab in the navigation bar. When set to Allow, users are allowed to list and manage printers.	Allow, Deny	Allow	No
Vary on/off printers	Controls whether Vary on and Vary off actions may be performed on a printer.	Allow, Deny	Allow	No
Start/stop change writers	Controls whether Start, Stop, and Change actions may be performed on a writer.	Allow, Deny	Allow	No
Printers list view	Controls which columns view (Basic or Advanced) to display when viewing printers.	Basic, Advanced	Basic	Yes
Printers list columns - Basic	Specifies which columns to display when Printers list view is set to Basic.	Any combination of and ordering of: Printer, Printer Status, Printer Action, Printer Description, Output Queue, Output Queue Status, Writer, Current File, Current User, Current File User Data, Current File Form Type	Printer, Printer Status, Printer Action, Printer Description, Output Queue	Yes
Printers list columns - Advanced	Specifies the identity and order of columns to display when Printers list view is set to Advanced.	Any combination of and ordering of: Printer, Printer Status, Printer Action, Output Queue, Output Queue Status, Writer, Writer Status, Writer Action, Printer Description, Current File, Current User, Current File User Data, Current File Form Type	Printer, Printer Status, Printer Action, Printer Description, Output Queue, Output Queue Status, Output Queue Action, Writer, Writer Status, Writer Action	Yes

Table 15. Print Policies (continued)

Policy	Description	Values	Default Values	Preference
Internet printers	Controls access to the Internet printers function, and whether the Internet printers item is available on the Print tab in the navigation bar. When set to Allow, users are allowed to list internet printers.	Allow, Deny	Allow	No
Internet printers list columns	Specifies the identity and order of the columns to be displayed when viewing Internet printers.	Internet Printer, Output Queue, URL, Printer Data Type, Printer File, Authentication Method	Internet Printer, Output Queue, URL, Printer Data Type, Printer File, Authentication Method	Yes
Printer shares	Controls access to the Printer shares function, and whether the Pinter shares item is available on the Print tab in the navigation bar. When set to Allow, users are allowed to list printer shares information.	Allow, Deny	Allow	No
Printer shares list columns	Specifies the identity and order of the columns to be displayed when viewing printer shares.	Share, Output Queue, Printer Driver, Spooled File Data Type, Users, Share Description	Share, Output Queue, Printer Driver, Spooled File Data Type, Users, Share Description	Yes
Output queues	Controls access to the Output queues function, and whether the Output queues item is available on the Print tab in the navigation bar. When set to Allow, users are allowed to list, manage and view status of output queues.	Allow, Deny	Allow	No
Display output queues contents	Controls whether the contents of any output queues can be displayed.	Allow, Deny	Allow	No
Hold/release output queues	Controls whether the Hold and Release actions may be performed on an output queue.	Allow, Deny	Allow	No
Output queue filter	Specifies the output queues that will be displayed when listing output queues.	Specific name, Generic name, or the special value *ALL.	*All	Yes
Output queue library filter	Specifies the libraries which are searched for output queues.	One of the following: <ul style="list-style-type: none"> • Use user portion of library list • Use all libraries • Use all user libraries • Use current library • Use library list 	Use user portion of library list	Yes
Output queue list columns	Specifies the identity and order of the columns to be displayed when viewing output queues.	Any combination of and ordering of: Output Queue, Status, Action, Files, Writer	Output Queue, Status, Action, Files, Writer	Yes

Messages

The following policies control access to the Messages tasks.

Table 16. Messages Policies

Policy	Description	Values	Default Value	Preference
Messages tab	Controls whether the Messages tab is visible in the navigation bar.	Show, Hide	Show	Yes
Display messages	Controls access to the Display messages function, and whether the Display messages item is available on the Messages tab in the navigation bar. When set to Allow, users are allowed to display, answer and manage messages in their message queue.	Allow, Deny	Allow	No
Delete messages	Controls whether the Delete action can be performed on a message in a message queue.	Allow, Deny	Allow	No
Reply to messages	Controls whether a message reply can be send in response to an inquiry type message.	Allow, Deny	Allow	No
Remove all messages	Controls whether the Remove All Messages option is available from the Display messages list.	Allow, Deny	Allow	No
Remove all answered messages	Controls whether the Remove All Answered Messages option is available from the Display messages list.	Allow, Deny	Allow	No
Display messages list columns	Specifies the identity and order of the columns to be displayed when viewing messages in a queue.	Any combination of and ordering of : ID, Message text, Type, Date/Time, Severity, Action	ID, Message text, Type, Date/Time, Severity, Action	Yes
Send Message	Controls access to the Send message function, and whether the Send message item is available on the Messages tab in the navigation bar. When set to Allow, users are allowed to send messages to a user or message queue.	Allow, Deny	Allow	No
Message queues	Controls access to the Message queues messages function, and whether the Message queues item is available on the Messages tab in the navigation bar. When set to Allow, users are allowed to display message queues and manage messages in those queues.	Allow, Deny	Allow	No
Display message queue contents	Controls whether the user can view and manage messages in other user's message queues.	Allow, Deny	Allow	No
Create message queue	Controls whether the Create message queue option is available from the Message queues list.	Allow, Deny	Allow	No

Table 16. Messages Policies (continued)

Policy	Description	Values	Default Value	Preference
Delete message queue	Controls whether the Delete message queue action is available from the Message queues list.	Allow, Deny	Allow	No
Message queue list columns	Specifies the identity and order of the columns to be displayed when viewing the Message queues list.	Any combination of and ordering of: Queue, Description, Action.	Queue, Description, Action	Yes

Jobs

The following policies control access to the Jobs tasks.

Table 17. Jobs Policies

Policy	Description	Values	Default Value	Preference
Jobs tab	Controls whether the Jobs tab is visible in the navigation bar.	Show, Hide	Show	Yes
Jobs	Controls access to the User jobs function, and whether the Jobs item is available on the Jobs tab in the navigation bar. When set to Allow, users are allowed to list and manage their user jobs running on the iSeries.	Allow, Deny	Allow	No
User job list filter	Specifies the types of user jobs to display by default based on the current job status.	One of the following: • All jobs • Active jobs • Active jobs and waiting to run • Jobs waiting to run • Completed jobs	Active jobs and waiting to run	Yes
User job list columns	Specifies the identity and order of the columns to be displayed when viewing user jobs.	Any combination of and ordering of: Job, Status, Type, Entered System, Action, User, Current User, Detailed Status, Function, Job Queue, Job Queue Library, Job User Identity, Memory Pool, Number, Output Queue, Output Queue Library, Priority on Job Queue, Priority on Output Queue, Run Priority, Subsystem, Subsystem Library, Thread Count, Total CPU DB Time, Total CPU Time	Job, Status, Type, Entered System, Action	Yes
User job actions	Controls whether any job actions (hold/release, delete/end, job log, printer output, properties) can be performed when viewing the user job list.	Allow, Deny	Allow	No
Job action prompt mode	Controls which prompt (Basic or Advanced) will be displayed when performing a hold or delete/end job action on a user job.	Basic, Advanced	Basic	No

Table 17. Jobs Policies (continued)

Policy	Description	Values	Default Value	Preference
Hold/Release jobs	Controls whether the Hold and Release actions can be performed on a user job.	Allow, Deny	Allow	No
Delete/end jobs	Controls whether the Delete/End action can be performed on a user job.	Allow, Deny	Allow	No
Display user job logs	Controls whether the view Job Log action can be performed on a user job.	Allow, Deny	Allow	No
User job log sort order	Specifies to sort the user job log in either ascending or descending order based on the date/time the messages were logged. Descending means the most recent messages logged will be displayed first.	Ascending, Descending	Descending	Yes
User job log columns	Specifies the identity and order of the columns to be displayed when viewing user job logs.	Any combination of and ordering of : ID, Message text, Type, Date/Time, Severity, From Program	ID, Message text, Type, Date/Time, Severity, From Program	Yes
Display user job properties	Controls whether the view Properties action can be performed on a user job.	Allow, Deny	Allow	No
Work with other user's jobs	Controls whether this user can work with other user's jobs. Note: By default, iSeries user profiles with *JOBCTL special authority are automatically allowed access to this function.	Allow, Deny	Deny	No
Server jobs	Controls access to the Server jobs function, and whether the Server jobs item is available on the Jobs tab in the navigation bar. When set to Allow, users are allowed to list and manage server jobs running on their behalf on the iSeries.	Allow, Deny	Allow	No
Server job list columns	Specifies the identity and order of the columns to be displayed when viewing server jobs.	Any combination of and ordering of: Job, Detailed Status, Server, Run Priority, Thread Count, Action, Current User, Entered System, Function, Job User Identity, Memory Pool, Number, Status, Subsystem, Subsystem Library, Total CPU DB Time, Total CPU Time, Type, User	Job, Detailed Status, Server, Run Priority, Thread Count, Action	Yes
Server job actions	Controls whether any job actions (hold/release, delete/end, job log, printer output, properties) can be performed when viewing the server job list.	Allow, Deny	Allow	No

Table 17. Jobs Policies (continued)

Policy	Description	Values	Default Value	Preference
Job action prompt mode	Controls which prompt (Basic or Advanced) will be displayed when performing a hold or delete/end job action on a server job.	Basic, Advanced	Basic	No
Hold/Release jobs	Controls whether the Hold and Release actions can be performed on a server job.	Allow, Deny	Allow	No
Delete/end jobs	Controls whether the Delete/End action can be performed on a server job.	Allow, Deny	Allow	No
Display server job logs	Controls whether the view Job Log action can be performed on a server job.	Allow, Deny	Allow	No
Server job log sort order	Specifies to sort the server job log in either ascending or descending order based on the date/time the messages were logged. Descending means the most recent messages logged will be displayed first.	Ascending, Descending	Descending	Yes
Server job log columns	Specifies the identity and order of the columns to be displayed when viewing server job logs.	Any combination of and ordering of : ID, Message text, Type, Date/Time, Severity, From Program	ID, Message text, Type, Date/Time, Severity, From Program	Yes
Display server job properties	Controls whether the view Properties action can be performed on a server job.	Allow, Deny	Allow	No
Work with other user's server jobs	Controls whether this user can work with other user's server jobs. Note: By default, iSeries user profiles with *JOBCTL special authority are automatically allowed access to this function.	Allow, Deny	Deny	No

5250

The following policies control access to the 5250 tasks.

Table 18. 5250 Policies

Policy	Description	Values	Default Value	Preference
5250 tab	Controls whether the 5250 tab is visible in the navigation bar.	Show, Hide	Show	Yes
Start 5250 sessions	Controls access to 5250 user interface sessions and specifies whether the Start session item is available on the 5250 tab in the navigation bar.	Allow, Deny	Allow	No

Database

The following policies control access to the Database tasks.

Table 19. Database Policies

Policy	Description	Values	Default Value	Preference
Database tab	Controls whether the Database tab is visible in the navigation bar.	Show, Hide	Show	Yes
Tables	Controls access to the Tables function, and whether the Tables item is available on the Database tab in the navigation bar. When set to Allow, users are allowed to retrieve the list of relational database tables on the iSeries server.	Allow, Deny	Allow	No
Maximum table rows	Specifies the maximum number of tables to return in the tables list.	50 - 10,000 or no maximum	500	Yes
Table filter	Specifies the tables to display in the Tables list.	Comma-separated list of schemas, schema filters, tables, and table filters. The % character is used as the filter character. *USRLIBL is a special value to identify all tables in the user portion of the library list. For example, QIWS,MYSHEMA.MYTABLE, T%,%.R% retrieves all tables in QIWS, the table MYSHEMA.MYTABLE, all tables in schemas beginning with T, and all tables beginning with R.	*USRLIBL	Yes, if "Table filter is user preference" is allowed
Table filter is user preference	Controls whether providing a table filter is supported as a user preference or as an administrator only controlled policy.	Allow, Deny	Allow	No
Insert records into table	Controls the ability to insert records into a database table using Insert Record. It does not control inserts using Run SQL.	Allow, Deny	Allow	No
Update records in table	Controls the ability to update and delete records from a database table, using Update Record. It does not control updates using Run SQL.	Allow, Deny	Allow	No
Quick view table records	Controls the ability to view the contents of a database table, using Quick View.	Allow, Deny	Allow	No
Maximum quick view rows	Specifies the maximum number of rows to return when viewing a database table.	50 - 10,000 or no maximum	1000	Yes

Table 19. Database Policies (continued)

Policy	Description	Values	Default Value	Preference
Requests	Controls access to the My Requests function, and whether the My Requests item is available on the Database tab in the navigation bar. When set to Allow, users are allowed to retrieve the list of database requests and shortcuts to which they have access.	Allow, Deny	Allow	No
Run request	Controls the ability to run saved SQL and copy data to table requests.	Allow, Deny	Allow	No
Copy request	Controls the ability to copy saved SQL and copy data to table requests.	Allow, Deny	Allow	No
Delete request	Controls the ability to delete saved SQL and copy data to table requests.	Allow, Deny	Allow	No
Rename request	Controls the ability to rename saved SQL and copy data to table requests.	Allow, Deny	Allow	No
Edit request	Controls the ability to edit saved SQL and copy data to table requests.	Allow, Deny	Allow	No
Save request	Controls the ability to save SQL and copy data to table requests.	Allow, Deny	Allow	No
List shortcuts	Controls the ability to retrieve the list of shortcuts created by the current user.	Allow, Deny	Allow	No
Create shortcut	Controls the ability to create shortcuts to saved SQL and copy data to table requests.	Allow, Deny	Allow	No
Copy shortcut	Controls the ability to copy requests accessed through shortcuts.	Allow, Deny	Allow	No
Delete shortcut	Controls the ability to delete shortcuts to saved SQL and copy data to table requests.	Allow, Deny	Allow	No
Rename shortcut	Controls the ability to rename shortcuts to saved SQL and copy data to table requests.	Allow, Deny	Allow	No
Request list columns	Specifies the identity and order of columns displayed when you view the My Requests list.	Any combination of and ordering of: Request, Description, Created by, Access, Action, Shortcut	Request, Description, Action, Shortcut, Created By, Access	Yes

Table 19. Database Policies (continued)

Policy	Description	Values	Default Value	Preference
Run SQL requests	Controls access to the Run SQL function, and whether the Run SQL item is available on the Database tab in the navigation bar. When set to Allow, users are allowed to invoke Run SQL and to use the SQL Wizard.	Allow, Deny	Allow	No
Run statements other than query	Controls the ability to run all types of SQL statements when using Run SQL or when running saved SQL requests. If this value is Deny, only statements which generate a single result set are allowed to run.	Allow, Deny	Allow	No
Copy data to table	Controls access to the Copy data to table function, and whether the Copy data to table item is available on the Database tab in the navigation bar. When set to Allow, users are allowed to copy data from a file to a database table.	Allow, Deny	Allow	No
Create new tables	Controls the ability to create a new database table when running a copy data to table request.	Allow, Deny	Allow	No
Append data to tables	Controls the ability to append data to an existing table when running a copy data to table request.	Allow, Deny	Allow	No
Replace data in tables	Controls the ability to replace the contents of a database table when running a copy data to table request.	Allow, Deny	Allow	No
Import request	Controls access to the Import request function, and whether the Import request item is available on the Database tab in the navigation bar. When set to Allow, users are allowed to import existing Client Access Database Transfer requests into iSeries Access for Web.	Allow, Deny	Allow	No
Default connection	Specifies the database connection to be used when making database requests.	Any connection defined in the database connection list.	IBM Toolbox for Java - server name	Yes, if "Default connection is user preference" is allowed.
Default connection is user preference	Controls whether selecting a default connection is supported as a user preference or as an administrator only controlled policy.	Allow, Deny	Allow	No

Table 19. Database Policies (continued)

Policy	Description	Values	Default Value	Preference
Add IBM Toolbox for Java to connection list	Controls whether an IBM Toolbox for Java connection should automatically be included in the list of available connections, when the database connection list is not empty. If the database connection list is empty, the IBM Toolbox for Java connection will always be included.	Allow, Deny	Allow	No

Files

The following policies control access to the Files tasks.

Table 20. Files Policies

Policy	Description	Values	Default Value	Preference
Files tab	Controls whether the Files tab is visible in the navigation bar.	Show, Hide	Show	Yes
Browse files	Controls access to the Browse files function, and whether the Browse files item is available on the Files tab in the navigation bar. When set to Allow, users are allowed to browse directories and files in the iSeries integrated file system.	Allow, Deny	Allow	No
Copy files to server	Controls whether users are allowed to copy files from their local file system to the currently displayed integrated file system directory.	Allow, Deny	Allow	No
Copy files from server	Controls whether users are allowed to copy files from the currently displayed integrated file system directory to their local file system.	Allow, Deny	Allow	No
Default directory	Specifies the directory to display by default when no other directory path is provided to the Browse files function.	A fully-qualified iSeries integrated file system path.	/	No
Display subdirectory contents	Controls whether subdirectories can have their contents displayed by navigating into them. This policy only applies to the right hand or list pane of the Browse files window.	Allow, Deny	Allow	No
Display parent directory contents	Controls whether the currently displayed directory can have its parent directory contents displayed by navigating back to the parent.	Allow, Deny	Allow	No

Table 20. Files Policies (continued)

Policy	Description	Values	Default Value	Preference
Display default directory parent contents	Controls whether the initially displayed directory can have its parent directory contents displayed by navigating back to the parent.	Allow, Deny	Deny	No
File directory contents columns	Specifies the identity and order of columns to be displayed when using the Browse files function.	Any combination of and ordering of: Name, Size, Type, Modified, Action.	Name, Size, Type, Modified, Action	Yes
File actions	Controls whether any file actions (create/rename/delete of directories and copy/rename/delete/mail of files) can be performed when using the Browse files function.	Allow, Deny	Allow	No
Create directories	Controls whether the create directory action can be performed when using the Browse files function.	Allow, Deny	Allow	No
Rename directories	Controls whether the rename directory action can be performed when using the Browse files function.	Allow, Deny	Allow	No
Delete directories	Controls whether the delete directory action can be performed when using the Browse files function.	Allow, Deny	Allow	No
Copy files	Controls whether the copy file action can be performed when using the Browse files function.	Allow, Deny	Allow	No
Rename files	Controls whether the rename file action can be performed when using the Browse files function.	Allow, Deny	Allow	No
Delete files	Controls whether the delete file action can be performed when using the Browse files function.	Allow, Deny	Allow	No
Mail files	Controls whether the mail file action can be performed when using the Browse files function.	Allow, Deny	Allow	No
File shares	Controls access to the File shares function, and whether the File shares item is available on the Files tab in the navigation bar. When set to Allow, users are allowed to browse the NetServer file shares defined on the iSeries.	Allow, Deny	Allow	No
Display file share contents	Controls whether contents of NetServer file shares can be displayed.	Allow, Deny	Allow	No
Shares list columns	Specifies the identity and order of columns to be displayed when viewing the list of defined NetServer file shares.	Any combination of and ordering of: Share Name, Description, User Count, Permission.	Share Name, Description, User Count, Permission	Yes

Table 20. Files Policies (continued)

Policy	Description	Values	Default Value	Preference
Copy files to server	Controls whether users are allowed to copy files from their local file system to the currently displayed NetServer file share directory.	Allow, Deny	Allow	No
Copy files from server	Controls whether users are allowed to copy files from the currently displayed NetServer file share directory to their local file system.	Allow, Deny	Allow	No
Default directory	Specifies the directory to display by default when no other directory path is provided to the File shares function.	Any valid iSeries NetShare File Share name	/QIBM	No
Display subdirectory contents	Controls whether subdirectories can have their contents displayed by navigating into them when browsing NetServer File Shares.	Allow, Deny	Allow	No
Display parent directory contents	Controls whether the currently displayed directory can have its parent directory contents displayed by navigating back to the parent when browsing NetServer File Shares.	Allow, Deny	Allow	No
Display default directory parent contents	Controls whether the initially displayed directory can have its parent directory contents displayed by navigating back to the parent when browsing NetServer File Shares.	Allow, Deny	Deny	No
Share directory contents columns	Specifies the identity and order of columns to be displayed when browsing NetServer File Shares.	Any combination of and ordering of: Name, Size, Type, Modified, Action.	Name, Size, Type, Modified, Action	Yes
File share actions	Controls whether any file actions (create/rename/delete of directories and copy/rename/delete/mail of files) can be performed when browsing NetServer File Shares.	Allow, Deny	Allow	No
Create directories	Controls whether the create directory action can be performed when browsing NetServer File Shares.	Allow, Deny	Allow	No
Rename directories	Controls whether the rename directory action can be performed when browsing NetServer File Shares.	Allow, Deny	Allow	No
Delete directories	Controls whether the delete directory action can be performed when browsing NetServer File Shares.	Allow, Deny	Allow	No

Table 20. Files Policies (continued)

Policy	Description	Values	Default Value	Preference
Copy files	Controls whether the copy file action can be performed when browsing NetServer File Shares.	Allow, Deny	Allow	No
Rename files	Controls whether the rename file action can be performed when browsing NetServer File Shares.	Allow, Deny	Allow	No
Delete files	Controls whether the delete file action can be performed when browsing NetServer File Shares.	Allow, Deny	Allow	No
Mail files	Controls whether the mail file action can be performed when browsing NetServer File Shares.	Allow, Deny	Allow	No

Command

The following policies control access to the Command tasks.

Table 21. Command Policies

Policy	Description	Values	Default Value	Preference
Command tab	Controls if the Command tab is shown in the navigation area of the page.	Show, Hide	Show	Yes
Run commands	Controls access to the Run command function, and whether the Run Command item is available on the Command tab in the navigation bar. When set to Allow, users are allowed to run iSeries commands. Note: Users with Limit Capabilities-*YES in their user profile will not be able to run commands with iSeries Access for Web regardless of this setting.	Allow, Deny	Allow	No
Number of previous commands remembered	Specifies the number of previously run, unique commands to be displayed by the Run command function. These commands are not remembered across browser sessions.	Any integer greater than or equal to 0	20	Yes
My commands	Controls access to the My commands function, and whether the My commands item is available on the Command tab in the navigation bar. When set to Allow, users are allowed to save previously run commands to their My Commands list.	Allow, Deny	Allow	No

Table 21. Command Policies (continued)

Policy	Description	Values	Default Value	Preference
Maximum commands user can save	Controls the maximum number of commands the user save in their My Commands list.	25 - 1000 or no maximum	No maximum	No
My commands list columns	Specifies the identity and order of columns to display in the My Commands list.	Any combination of and ordering of: Name, Command, Output, Action, Last access	Name, Command, Output, Action, Last access	Yes
My commands sort column	Specifies the column to sort on when displaying the My Commands list.	Name, Command, Output, Last access	Name	Yes
My commands sort order	Specifies the order to sort commands (based on the sort column) when displaying the My Commands list.	Ascending, Descending	Ascending	Yes
Maximum characters to display in Command column	Specifies the maximum number of characters to show in the Command column when displaying the My Commands list.	10 - 1000 or no maximum	No maximum	Yes
Search for commands	Controls access to the Search for commands function, and whether the Search item is available on the Command tab in the navigation bar. When set to Allow, users are allowed to search for iSeries commands by command name or text description.	Allow, Deny	Allow	No
Default search library	Specifies the libraries to look in when using the Search for commands function.	One of the following: • *LIBL - searches for commands in the libraries in your user library list. • *ALL - searches for commands in all libraries on the iSeries. • Library name - searches for commands in the specified library. Only one library may be specified and wildcards are not allowed.	*LIBL	Yes
Search for commands by	Specifies the default search mode that will be selected when using the Search for commands function.	One of the following: • Command name: search for command names that match the pattern specified in the command field. • Text description: search for command names whose text description contains any of the words specified in the command field.	Command name	Yes

Mail

The following policies control access to the Mail tasks.

Table 22. Mail Policies

Policy	Description	Values	Default Value	Preference
Send mail	Controls access to the Send mail function. When set to Allow, users are allowed to send items such as PDF output, SQL results, and integrated file system files as e-mail attachments.	Allow, Deny	Allow	No
SMTP mail server	Specifies the SMTP mail server to use for the Send mail function. Normally, this server name would be configured at the *PUBLIC group setting level. Note: The send mail options are not available to users until a SMTP server name is configured.	Any valid SMTP mail server name	None	No
E-mail address	Specifies the e-mail address that will be used in the From field on the e-mail attachment settings page. Note: The send mail options are not available to a user until an e-mail address is configured.	Any valid e-mail address	None	Yes, when "E-mail address is user preference" is allowed.
E-mail address is user preference	Controls whether providing an e-mail address is supported as a user preference or as an administrator only controlled policy.	Allow, Deny	Allow	No

My Folder

The following policies control access to the My Folder tasks.

Table 23. My Folder Policies

Policy	Description	Values	Default Value	Preference
My Folder link	Controls whether the My Folder link is visible in the navigation bar.	Show, Hide	Show	Yes
My Folder	Controls access to the My Folder function. When set to Allow, users are allowed to work with items sent to their personal folder.	Allow, Deny	Allow	No
Create folder items	Controls whether this user is allowed to create new folder items in another user's personal folder.	Allow, Deny	Allow	No
Send e-mail on new folder items	Controls whether an e-mail notification should be sent to the folder owner when new items are put into their personal folder.	Yes, No	Yes	Yes

Table 23. My Folder Policies (continued)

Policy	Description	Values	Default Value	Preference
E-mail address to notify	Specifies the e-mail address to notify when new items are put into the user's personal folder.	Any valid e-mail address	Defaults to user's Mail->E-mail address preference, if one is not specified here.	Yes
My Folder columns	Specifies the identity and order of columns to display in the My Folder list	Any combination of and ordering of Item, Status, From, Date/Time, Size, Action	Item, Status, From, Date/Time, Size, Action	Yes
My Folder sort column	Specifies the column to sort on when displaying the My Folder list.	Item, Status, From, Date/Time, Size	Date/Time	Yes
My Folder sort order	Specifies the order to sort folder items (based on sort column) when displaying the My Folder list.	Ascending, Descending	Descending	Yes

Administration

The following policies control access to the Customize tasks.

Table 24. Customize Policies

Policy	Description	Values	Default Value	Preference
Customize tab	Controls whether the Customize tab is visible in the navigation bar.	Show, Hide	Show	Yes

Table 24. Customize Policies (continued)

Policy	Description	Values	Default Value	Preference
Grant administrator privileges	<p>Controls access to the policy administration functions, and whether the User Profiles, Group Profiles, and Selected Profile items are available on the Customize tab in the navigation bar. When set to Allow, the user is allowed to change and save iSeries Access for Web policy settings for other iSeries user and group profiles. By default, iSeries user profiles with *SECADM special authority are automatically allowed access these functions.</p> <p>Note: Users given this authority will only be able to change policy settings for iSeries user and group profiles that they have at least *CHANGE object authority to. This setting allows users with *SECADM special authority to grant other user profiles access to this function without the need to also grant them *SECADM special authority on the iSeries.</p> <p>Also controls access to the connection pool and trace functions, and whether the Connection pool and Trace items are available on the Other tab in the navigation bar. When set to Allow, the user is allowed to change connection pool properties and use the trace function.</p>	Allow, Deny	Deny	No
Edit public settings	<p>Controls whether the user is allowed to change and save the iSeries Access for Web *PUBLIC group policy settings. These public settings are defined as the default settings for all user and groups, meaning these policy settings will be enforced when a user does not have the corresponding policy defined for their user profile or any of their group profiles memberships.</p> <p>Note: *PUBLIC group settings are accessed from the Customize Group Profiles list. The user must first be granted administrator privileges in order for this policy to take affect.</p>	Allow, Deny	Deny	No

Table 24. Customize Policies (continued)

Policy	Description	Values	Default Value	Preference
Edit preferences	Controls access to the Preferences function, and whether the Preferences item is available on the Customize tab in the navigation bar. When set to Allow, users are allowed to change and save preferences for their user profile. These preferences are remembered across iSeries Access for Web browser sessions, and will be used every time the user logs in.	Allow, Deny	Allow	No

Other

The following policies control access to Other tasks.

Table 25. Other Policies

Policy	Description	Values	Default Value	Preference
Other tab	Controls whether the Other tab is visible in the navigation bar.	Show, Hide	Show	Yes
Change password	Controls access to changing your password and specifies whether the Change password item is available on the Other tab in the navigation bar.	Allow, Deny	Allow	No
About Access for Web	Controls access to information about iSeries Access for Web and specifies whether the About item is available on the Other tab in the navigation bar.	Allow, Deny	Allow	No
Display software product list	Controls access to displaying the list of currently installed software products on the iSeries and whether a link to this information is provided on the About Access for Web page.	Allow, Deny	Allow	No
Display software product information	Controls whether links to detailed information about software products are available from the software product list.	Allow, Deny	Allow	No
Display software fix list	Controls whether a link to the software fix list is available from the detailed software product information page.	Allow, Deny	Allow	No
Display software fix information	Controls whether links to detailed information about software product fixes are available from the software fix list.	Allow, Deny	Allow	No

Table 25. Other Policies (continued)

Policy	Description	Values	Default Value	Preference
Display system values	Controls access to displaying the current settings for iSeries system values and whether a link to this information is provided on the About Access for Web page.	Allow, Deny	Allow	No

Chapter 8. Preferences

Introduction

iSeries Access for Web provides a Preferences function which allows users to customize iSeries Access for Web settings to meet their needs. By default, all users are allowed to modify their preferences. Any preference modifications will be saved and associated with their iSeries user profile.

Preferences are actually a subset of the complete list of policy settings available. Refer to the policy tables in Chapter 7, "iSeries Access for Web Policies" on page 75 for the complete list of user preferences.

Categories of Preferences

Users can set the following types of preferences:

- Column inclusion and ordering for functions that display output in columns.
- Number of rows per page to display on output.
- Show or hide navigation bar tabs.
- Preferred language and character set.
- Database table filters and default database connection.
- Number of commands to save in the run command history.

Use Preferences

When you select the Preferences function, a panel provides a list of preference links organized by functional category. Selecting a link displays a table of preference settings specific to that function. Each row in the table contains the preference name, its current setting, where the setting is being derived from, and the available actions to be performed. For additional information on the "derived from" column, see Chapter 9, "Administering Users and Groups" on page 101. You can perform up to three actions for each preference setting:

Table 26.

Action	Description
Use current setting	This is the default action that is pre-selected. If the setting is not modified, no action is performed. If the setting is modified, it will be added to your user profile record in the iSeries Access for Web policies file.
Apply setting to profile	Select this action to add the current setting to your user profile record in the iSeries Access for Web policies file. The setting will be written to your user profile record, even if it was not modified. You would use this action to ensure you get this preference. This is because a different preference may be used based on whether you are a member of any iSeries group profiles.
Reset to default	Select this action to remove the setting from your user profile record in the iSeries Access for Web policies file. This option is only available if your user profile record currently contains a specific value for this preference. Removing the preference will mean you will inherit this setting from a group profile, either a specific group or the public group setting.

Restrict Access to Preferences

Administrators can deny specific users or groups access to the Preferences function. This is controlled by an administration policy called "Edit preferences". This policy is useful in organizations where administrators want to set up all customization options for users and ensure users are not able to modify any preference settings. See "Administration" on page 94 for information on the Edit preferences policy setting.

Chapter 9. Administering Users and Groups

Introduction

iSeries Access for Web provides a Customize function for administrators to set policies for user and group profiles. These policies allow administrators to control what functions a user can perform and how certain information will be presented. When a function is restricted, its navigation bar content will be removed. Restricting a function also restricts access to the corresponding servlet. This means the function is also restricted if a user tries to access the servlet directly via its URL. When an administrator sets policies for a user or group, they take effect immediately.

Who Can Administer Other Users and Groups

Administrators with *SECADM special authority in their iSeries user profile are automatically authorized to administer iSeries Access for Web settings for other users and groups. These administrators, in turn, have authority to grant other user profiles permission to the iSeries Access for Web administration functions. This is accomplished by setting the "Grant administrator privileges" policy for that user. See "Administration" on page 94 for additional information on this policy. In either case, the administrator can only update policy settings for iSeries profiles that they have authority to.

Determine Policy Settings for a User

It is important for administrators to know how policy settings for an individual user are determined. The following sequence of checks are made when a policy related decision needs to be made for the logged on user:

1. If the policy setting is specific to the user profile, it will be enforced.
2. If the policy setting is not specific to the user profile, group profiles that the user is a member of are checked. If the policy has been set for any of these group profiles, it will be enforced.
3. If the policy setting is not found in any of the user's group profiles, a special group, *PUBLIC is checked. If the policy has been set in the *PUBLIC group profile, it will be enforced.
4. If the policy setting is not found in the user's profile, any group profiles, or the *PUBLIC group profile, the shipped default policy setting will be used.

The described sequence can be viewed more easily as the following:

1. User profile
2. Group profile(s)
3. Administrator-supplied user defaults (*PUBLIC profile - UserData policy file)
4. IBM-supplied defaults (*PUBLIC profile - ProdData policy file)

The "Derived From" column (displayed when editing policy and preference settings) indicates where in the above search order the policy was found.

Customize User Profiles

This function provides an administrator with a list of iSeries user profiles they are authorized to customize. This list reflects the same set of user profiles they would have access to from the iSeries Work with User Profiles (WRKUSRPRF) command. Administrators with *ALLOBJ special authority would have access to all user profiles.

The administrator can perform up to three actions for each user profile:

Table 27. Customize User Profile Actions

Action	Description
Edit	This action is always available. Use this option to create or modify policy settings for the specified user or group profile.
Copy	This action is only available when the user or group profile currently has policy settings. It allows you to copy all of the policy settings from this profile to one or more other profiles.
Reset	This action is only available when the user or group profile currently has policy settings. It allows you to remove all of the policy settings specific to this profile.

Selecting the Edit action displays a table of links organized by functional category. Selecting a link will display a table of policy settings specific to that function. Each row in the policy table contains the policy name, its current setting, where the setting is being derived from, and the available actions to be performed.

There are at most three actions the administrator can perform for each policy setting:

Table 28. Policy Setting Actions

Action	Description
Use current setting	This is the default action that is pre-selected. If the setting is not modified, no action is performed. If the setting is modified, it will be added to the user or group profile record in the iSeries Access for Web policies file.
Apply setting to profile	Select this action to add the current setting to the user or group profile record in the iSeries Access for Web policies file. The setting will be written to the user or group profile record, even if it was not modified. You would use this action to ensure the user or group profile gets this setting. This is because a different policy setting may be used based on the user profile being a member of one or more iSeries group profiles.
Reset to default	Select this action to remove the setting from the user or group profile record in the iSeries Access for Web policies file. This option is only available if the user or group profile record currently contains a specific setting for this policy.

The "Derived From" column (displayed when editing policy and preference settings) indicates where the policy setting used for this user profile was found.

Table 29. "Derived From" Column Descriptions

Derived From	Description
Profile setting	Indicates the setting is currently specific to the profile being customized. The setting had previously been applied to this profile.

Table 29. "Derived From" Column Descriptions (continued)

Derived From	Description
Group - (groupName)	Indicates the setting is not specific to the profile being customized, but is being derived from the specified iSeries group profile and the user is a member of this group.
*PUBLIC setting	Indicates the setting is not specific to the profile being customized. No setting was found in any iSeries group profile memberships. The setting is being derived from the *PUBLIC group settings. This is a special group profile available to iSeries Access for Web administrators. All user profiles are automatically members of this special group profile. Administrators can modify this group profile to easily apply settings to all iSeries Access for Web users.
Shipped default	Indicates the setting is not specific to the profile being customized, no setting was found in any iSeries group profile memberships, or the special *PUBLIC group profile. The setting is being derived from a shipped default value.

Deny Access to Functions

Policy settings are grouped by function, with subfunction policies. Subfunction policies are visually indented in the customize panels to reflect this hierarchy. To deny access to a function, you just have to set the function setting to deny. You do not also have to explicitly deny all of the subfunctions.

Customize Group Profiles

This function provides an administrator with a list of iSeries group profiles they are authorized to customize. This list reflects the same set of group profiles they have access to from the iSeries Work with User Profiles (WRKUSRPRF) command. Administrators with *ALLOBJ special authority would have access to all group profiles. The user interface for updating and setting policies for group profiles is identical to setting policies for individual user profiles.

*PUBLIC Group Settings

If the administrator is authorized, a special group profile (*PUBLIC) is available in the Customize Group Profiles list. It will be displayed as the first group profile in the list. This group profile can be used to customize settings that will be used by all user profiles on your iSeries. By definition, all users are members of this group and cannot be removed.

Copying Policy Settings to Other Profiles

The Customize User Profiles and Customize Group Profiles provide an easy way to replicate settings to other user or group profiles. After a user or group profile is customized by an administrator, a Copy action is available when viewing this profile in the list. Using this option, you can copy a complete set of policy settings from one user profile to one or more other profiles.

Strategies for Customizing iSeries Access for Web

iSeries Access for Web ships with a set of default policy settings. The default policy settings allow most of the iSeries Access for Web functions to be available for all users. Without any customization, users accessing iSeries Access for Web could begin using most of the available functions. As an administrator of this product, you may not want your users to be able to access all of these functions. It is the responsibility of an administrator to restrict functions they do not want their users to be able to access.

One of the quickest strategies that can be deployed to restrict a function from all users is to use the Customize Group Profiles function and customize the *PUBLIC group profile. This group profile is defined such that every user is a member of this group. So, for example, if you were to customize the *PUBLIC profile and set the "Browse files" and "File shares" file functions to "Deny", you would restrict file system access from this product for all users. If some of your users required access to this function, you could specifically customize their user profiles and set this function back to "Allow". In this way, only users that have been specifically allowed access will be able to use that function, all others would not have access.

Chapter 10. Customize the Home Page and Template File

iSeries Access for Web delivers a default home page that is shown when users go to the iWAHome URL. The default home page is designed to be a starting point to highlight the functions of the product, but is also meant to be an example of how to build your own home page or pages that access iSeries Access for Web functionality. The default home page can be replaced by using the Customize function to specify a completely different HTML file to be used for the home page. This home page replacement can be done for all users (*PUBLIC), or can be changed only for certain users and/or groups of users.

To specify that a different HTML file be used as the default home page do the following:

1. Select the **Customize** tab on the navigation bar.
2. Click **Selected profile**.
3. Type a user or group profile name into the text field.
4. Click **Customize Profile**.
5. Click the **General**.
6. In the Home page HTML file policy row, do the following:
 - a. Select **Apply Settings to Profile** from the pull down menu.
 - b. Replace the default home page file name with the file name you want used as your home page.
7. Click **OK** to replace the default home page with the html file you specified.
8. Click **My home page**, located at the top of the navigation bar, to verify that your default home page has been replaced.

If you don't need a drastic change to the home page look, you can also make a copy of and modify the default home page HTML file
/QIBM/ProdData/Access/Web2/html/homepage.html

Notes:

1. Do not place the new home page HTML file in the /QIBM/ProdData/Access/Web2 directory. This directory is meant for product files only. Place the home page file under the /QIBM/UserData/Access/Web2 tree, or in any location in the iSeries integrated files system.
2. *PUBLIC, QEJBSVR (for WebSphere), or QTMHHTTP (for Tomcat) must have at least *RX authority to the directory and user-defined HTML file.
3. If images are served as part of the user-defined home page, you must configure the HTTP server to serve the image files. Do not place the image files in the /QIBM/ProdData/Access/Web2/html/images directory. This directory is meant for product image files only.

With either option, the home page HTML file can also contain a `%%include list=file%%` tag. An example, `%%include list=/QIBM/ProdData/Access/Web2/config/info.policies%%`, can be found in the homepage.html file. This tag, found within a table definition, points to a file containing home page links to be included as link list items in a table. The list of items to include can be tailored for all users (*PUBLIC), groups of users, or individual users. This tag does not need to be present in a home page HTML file.

Other special tags that are also supported in the home page file are:

- `%%TITLE%%` - Replaced with title of the page

- %%USER%% - Replaced with the authenticated user name
- %%SYSTEM%% - Replaced with name of iSeries being accessed
- %%VERSION%% - Replaced with version of iSeries Access for Web that is installed

iSeries Access for Web also delivers a default look for its functional pages. The default look is controlled by a template file. The default template file is located in /QIBM/ProdData/Access/Web2/html/webaccess.html. Like the home page file, the template file that is used is also controlled by the Customization function and can be controlled at the *PUBLIC, group, and individual user level.

The template file has sections to specify the header and the footer areas of each of the functional pages, and where the iSeries Access for Web content is placed in the page. In addition to the 4 special tags listed above for the home page file, the template file also supports an additional special tag.

- %%CONTENT%% - Replaced with the functional content for the page

Part 5. Appendixes

Appendix A. Sources of Information for iSeries Access for Web

There are several places you can find additional information about iSeries Access for Web.

Information Authorized Program Analysis Report (Information APAR) and PTF

An **Information Authorized Program Analysis Report (Information APAR)** is an electronic document that is used to communicate information not found in publications, online information, critical fix information, or other sources.

Information APARs for iSeries Access for Web are available on the Internet or from the IBM fax information service. If you have Internet access, you can view the index to iSeries Access for Web Information APARs at:
<http://www.ibm.com/eserver/iseries/access/web/infoapars.htm>

Program temporary fixes (PTFs) are available to ensure that you have the latest program fixes for OS/400 and iSeries Access for Web.

You can also get the APARs and PTFs for iSeries Access for Web by using the Electronic Customer Support feature on your iSeries server. You need to have Electronic Customer Support configured and operational.

You can order informational APARs just like a PTF. You will receive a cover letter that contains all of the information in the APAR, however, no code or 'fix' comes with it.

To order an Information APAR, use the following OS/400 command: SNDPTFORD PTFID(IIxxxxx) where IIxxxxx is the APAR number.

After you load the APAR on the iSeries server, display or print it using the following command: DSPPTF LICPGM(INFOAS4)

For example, if iSeries Access for Web had information APAR II12345 which you have ordered and loaded on the iSeries server, use the following command to display it: DSPPTF LICPGM(INFOAS4)

Look for II12345. When you find it, use Option 5 to display.

Using the SNDPTFORD command requires Electronic Customer Support to be enabled on your iSeries server. If electronic customer support is not enabled, order the Information APAR the way that you normally get PTFs.

If you are not sure if an APAR is on your iSeries server, use the following to display all APARs:

1. Start Programming Development Manager (STRPDM)
2. Work with Members
3. File(QAPZCOVER), Library(QGPL), Name and Type(*ALL)

iSeries Access for Web Information on the Web

Other places you may want to get information from are listed in the following table, along with their web page addresses.

Table 30. Web Page Addresses Related to iSeries Access for Web

Web Page Address	Title
http://www.ibm.com	IBM Home Page
http://www.ibm.com/eserver/iseries	IBM iSeries Home Page
http://www.ibm.com/eserver/iseries/access/web/	IBM iSeries Access for Web Home Page
http://www.ibm.com/eserver/iseries/access	IBM iSeries Access Home Page
http://www.ibm.com/eserver/iseries/oper_nav IBM	iSeries Navigator Home Page
http://www.ibm.com/eserver/iseries/netserver	IBM AS/400 NetServer Home Page
http://www.ibm.com/software	IBM Software Home Page
http://www.ibm.com/eserver/iseries/support/	IBM AS/400 Service Home Page
http://www.ibm.com/eserver/iseries/access/hostpublisher http://www.ibm.com/software/webservers/hostpublisher	IBM WebSphere Host Publisher
http://www.redbooks.ibm.com	IBM Redbooks Home Page

IBM has a wealth of information on the Internet. The iSeries Information Center contains many articles about the iSeries server. It also contains links to the Information Center: Supplemental Manuals site (replaces the Online Library site) and the IBM home page. The Information Center can be accessed at:
<http://www.ibm.com/eserver/iseries/infocenter>.

iSeries Access for Web Read Me File

Refer to <http://www.ibm.com/eserver/iseries/access/web/readme.htm> for important information or technical changes to the product that were too late to include in the documentation.

Appendix B. Save and Restore

iSeries Access for Web

iSeries Access for Web can be propagated to other iSeries servers but there are considerations that need to be reviewed before saving and restoring iSeries Access for Web.

iSeries Access for Web can be saved and restored to other iSeries servers using the SAVLICPGM and RSTLICPGM commands. Using these commands has the same effect as installing iSeries Access for Web using the install media (CD-ROM) but the advantage is that any PTFs that have been applied are saved from the source server and restored to the target server.

After running the RSTLICPGM command, iSeries Access for Web must first be configured and started before it can be used. For more information, see Chapter 2, “iSeries Access for Web Setup Checklist” on page 7.

SAVLICPGM and RSTLICPGM will not save any user generated data. If user data needs to be propagated to other servers, the file system /QIBM/UserData/Access/Web2 directory needs to be saved and restored after iSeries Access for Web has been restored to a target server.

Appendix C. NLS Considerations

iSeries Access for Web displays information from a variety of sources. These sources include:

- OS/400
- JDBC driver
- WebSphere Application Server
- iSeries Access for Web

Some of these sources are able to provide information in more than one language, or format information in a language-specific manner. Such language-specific information includes forms, error messages, help, formatted dates and times, and sorted lists. When a choice of languages is available, every attempt is made to select a language that is appropriate for the user. The selected language is used to influence the language and format of information from these other sources. However, there is no guarantee that the information from a specific source will be in the selected language, or that all the information will be in the same language.

Messages and help which originate from OS/400 may not be in the selected language, depending on which language versions are installed on the iSeries. If the selected language is not installed on the iSeries, then OS/400 messages displayed by iSeries Access for Web will be in the primary language of the OS/400.

Language and Character Set Selection

iSeries Access for Web uses the following method in an attempt to select an appropriate language and character set.

First, a list of potential language choices is assembled from the following sources:

- iSeries Access for Web "Preferred language" policy
- Browser language configuration
- iSeries user profile Language ID
- Java Virtual Machine default locale

Second, the iSeries Access for Web "Preferred character set" policy is examined.

If a preferred character set was specified, then the list of potential languages is searched to find the first language that is compatible with the preferred character set. If a match is not found, then the preferred character set is not compatible with any of the potential languages so a default language and character set will be used.

If a preferred character set was not specified, then the first language from the list is selected, and a character set compatible with the selected language is chosen.

Information in Multiple Languages (Multilingual)

Because the information displayed by iSeries Access for Web comes from a variety of sources, there is the possibility that the information is in more than one language. When multiple languages are displayed in a browser simultaneously, a multilingual character set, such as UTF-8, may be required to display all the characters correctly. If this is the case, the "Preferred character set" policy should be changed to "Multilingual [UTF-8]".

CCSIDs and OS/400 Messages

To ensure that information is displayed properly, make certain that the Coded Character Set ID (CCSID) setting for the user profile is appropriate for the messages originating from OS/400.

Appendix D. Enrolling Users if You Use Document Library Services File System (QDLS)

Complete this procedure if you want to use the Document Library Services (QDLS) file system. To enroll iSeries Access users on the iSeries server follow these steps:

1. Type GO PCSTSK at the iSeries command prompt.
2. Select the Enroll Client Access Users option.

```
PCSTSK Client Access Tasks
System: SYSTEM1
Select one of the following:

User Tasks
1. Copy PC document to database
2. Copy database to PC document

Administrator Tasks
20. Work with Client Access administrators
21. Enroll Client Access users
```

3. Enter the appropriate information for:
 - User profile (name)
 - User ID (usually the same as the User profile name)
 - User address (usually the same as the iSeries server name)
 - User description
 - Add to system directory (use *YES if you want to use the QDLS file system)

See the online help for a complete description of the entry fields

```
Enroll Client Access Users

Type choices, press Enter.
User profile . . . . . AARON Name
User identifier:
User ID . . . . . AARON Character value
Address . . . . . SYSTEM1 Character value
User description . . . . . AARON B.
Add to system directory . . *NO *NO, *YES
```

4. Repeat steps 1-3 to enroll other users in the Directory Entry Database.

Appendix E. CL Commands used with iSeries Access for Web

When iSeries Access for Web was installed several CL commands were installed to library QIWA2. These commands should be used to perform actions such as configuring, starting, ending, and removing the iSeries Access for Web configuration within the web application sever.

The iSeries Access for Web CL commands are:

- CFGACCWEB2—Configure the iSeries Access for Web application server.
- STRACCWEB2—Start the iSeries Access for Web application server.
- ENDACCWEB2—End the running iSeries Access for Web application server.
- RMVACCWEB2—Remove the iSeries Access for Web application server configuration.

CFGACCWEB2 (Configure iSeries Access for Web) Command

Where allowed to run: All environments (*ALL)

Threadsafte: No

The Configure iSeries Access for Web (CFGACCWEB2) command is used to configure iSeries Access for Web for the web application server, either IBM WebSphere Application Server or Apache Software Foundation (ASF) Tomcat.

Before iSeries Access for Web can be used, it must be configured using this command.

Input parameters are conditional based on the value entered for the 'Web application server type' (APPSVRTYPE) parameter. After entering a value for the 'Web application server type' (APPSVRTYPE) parameter, press the F10 function key to display the additional parameters.

This command will use the input configuration parameters to add iSeries Access for Web servlet configuration information to the web application server.

If multiple web application servers, and instances of those application servers, are configured and running on the iSeries server, iSeries Access for Web can be configured to run within each of those web application servers and their instances.

When configuring iSeries Access for Web for multiple web application servers and instances, the new configuration can be created based on an existing configuration. The new configuration can share user generated data with other configurations or a copy of the existing user data can be made for the new configuration.

This command will create a directory structure for user generated data. User data will be stored to the the following locations depending on the value specified in the 'Web application server type' (APPSVRTYPE) parameter:

- *WAS40ADV - /QIBM/UserData/Access/Web2/was40adv/<instance_name>
- *WAS40SNG - /QIBM/UserData/Access/Web2/was40sng/<instance_name>
- *ASFTOMCAT - /QIBM/UserData/Access/Web2/asftomcat/<server_name>

When the command runs, a Java Shell Display session starts. Status information displays, indicating what the command is processing. As the command runs,

detailed status and error information is logged to /QIBM/UserData/Access/Web2/logs/cmds.log.

After the command completes, the web application server may have to be ended and restarted. The iSeries Access for Web configuration will need to be started before it can be accessed.

Associated commands:

- STRACCWEB2—Start Access for Web
- ENDACCWEB2—End Access for Web
- RMVACCWEB2—Remove Access for Web

Restrictions for CFGACCWEB2

1. The user of this command must have *ALLOBJ authority.
2. WebSphere Advanced Edition specific restrictions
 - The WebSphere Application Server subsystem must be running and in a ready state before running this command. Refer to the WebSphere documentation for information on starting the WebSphere subsystem and determining when it reaches a ready state.
 - If CFGACCWEB2 is run multiple times to change configuration information, the iSeries Access for Web configuration should be ended and restarted to ensure the configuration information is reloaded. Use the End Access for Web (ENDACCWEB2) and Start Access for Web (STRACCWEB2) commands or the web application server's administration function to end and restart iSeries Access for Web.
3. WebSphere Advanced Single Server Edition specific restrictions
 - The WebSphere Advanced Single Server Edition server must be ended and restarted after running Configure Access for Web (CFGACCWEB2).
4. ASF Tomcat specific restrictions
 - The ASF Tomcat server must be ended and restarted after running Configure Access for Web (CFGACCWEB2).

Parameters for CFGACCWEB2

This section contains information on the required and optional parameters for CFGACCWEB2.

Note: A bold, underlined value is the default value.

Table 31. CFGACCWEB2 Parameters

Keyword	Description	Choices	Notes
APPSVRTYPE	Web application server type	<i>Character value</i> , *WAS40ADV, *WAS40SNG, *ASFTOMCAT	Required
PORT	Servlet engine port number	<i>Character value</i>	Optional
WASINST	Web server instance name	<i>Character value</i> , <u>*DEFAULT</u>	Optional
TCSVRNAME	Tomcat server name	<i>Character value</i>	Optional
TCHMOEDIR	Tomcat home	<i>Path name</i>	Optional
TCUSRPRF	Tomcat user profile	<i>Character value</i>	Optional
SRCSVRTYPE	Source web server type	<i>Character value</i> , *WAS40ADV, *WAS40SNG, *ASFTOMCAT	Optional
SRCSVRINST	Source web server instance	<i>Character value</i> , *DEFAULT	Optional
SHRUSRDTA	Share user data	*NO, *YES	Optional

Web application server type (APPSVRTYPE)

Specifies which web application server to configure iSeries Access for Web to run under.

This is a required parameter.

Possible values are:

- ***WAS40ADV**: WebSphere 4.0 Advanced Edition is the web application server to be configured.
- ***WAS40SNG**: WebSphere 4.0 Advanced Single Server Edition is the web application server to be configured.
- ***ASFTOMCAT**: Apache Software Foundation Tomcat is the web application server to be configured.

Servlet engine port number (PORT)

Specifies the TCP/IP port number for the iSeries Access for Web web container to use. The port specified must be one that is not already being used by another application.

This parameter is a required and applicable only when configuring for the WebSphere Advanced Edition (*WAS40ADV) web application server.

For information on determining an available port number, see “Preparation for creating the HTTP Server” on page 18. After identifying a port number, the port number chosen should be added to the service table. Adding the chosen port number to the table may prevent future collisions with the chosen port number.

Web server instance name (WASINST)

Specifies which IBM WebSphere Application Server administrative server to configure to run iSeries Access for Web.

This value is only applicable when the ‘Web application server type’ (APPSVRTYPE) parameter is set to configure for WebSphere Advanced (*WAS40ADV) or Advanced Single Server (*WAS40SNG) Edition web application servers.

Possible values are:

- ***DEFAULT**: When IBM WebSphere Application Server was installed, a default administrative server was automatically created. When *DEFAULT is specified, iSeries Access for Web will be configured within the default WebSphere administrative server.
- **Web server instance name**: Specify the name of the WebSphere administrative server to configure to run iSeries Access for Web. This is the same administrative server name that was used when the WebSphere administrative server was created.

Tomcat server name (TCSRVNAME)

This value specifies the name of an existing ASF Tomcat server that will be configured to run iSeries Access for Web.

This value is required and applicable only when the ‘Web application server type’ (APPSVRTYPE) parameter is set to configure for the ASF Tomcat (*ASFTOMCAT) web application server.

Tomcat home directory (TCHOMEDIR)

This value specifies the ASF Tomcat home directory that the ASF Tomcat server was configured to use.

When the ASF Tomcat server was configured an integrated file system (IFS) path was specified as the location for the ASF Tomcat servlet engine

and its associated files. By default, the directory may have been set to /AFSTomcat/<server_name>. The path can be verified by checking the Tomcat server settings.

This home directory contains subdirectories for logs, applications, and configuration information for the ASF Tomcat server.

The Configure Access for Web (CFGACCWEB2) command will create directories and files within this path for iSeries Access for Web.

This value is required and applicable only when the 'Web application server type' (APPSVRTYPE) parameter is set to configure the ASF Tomcat (*ASFTOMCAT) web application server.

Tomcat user profile (TCUSRPRF)

This value specifies the user ID that the ASF Tomcat server was configured to use.

The Configure Access for Web (CFGACCWEB2) command will use this value to grant the ASF Tomcat server user ID access to iSeries Access for Web files.

This value is required and applicable only when the 'Web application server type' (APPSVRTYPE) parameter is set to configure the ASF Tomcat (*ASFTOMCAT) web application server.

Source web server type (SRCSVRTYPE)

When configuring iSeries Access for Web the configuration can be created based on an existing iSeries Access for Web configuration.

This value specifies a web application server that has been configured to run iSeries Access for Web.

This parameter is optional.

Possible values are:

- *WAS40ADV: WebSphere 4.0 Advanced Edition is a web application server that has been configured to run iSeries Access for Web.
- *WAS40SNG: WebSphere 4.0 Advanced Single Server Edition is a web application server that has been configured to run iSeries Access for Web.
- *ASFTOMCAT: Apache Software Foundation Tomcat is a web application server that has been configured to run iSeries Access for Web

Source web server instance (SRCSVRINST)

Specifies a WebSphere administrative server name or an ASF Tomcat server name that is configured within the web application server specified in the 'Source web server type'(SRCSVRTYPE) parameter. The new configuration's user data will be created based on this existing configuration.

This value is used in conjunction with the 'Source web server type' (SRCSVRTYPE) parameter.

Possible values for WebSphere are:

- *DEFAULT: When the web application server was installed, a default administrative server-instance was automatically created. When *DEFAULT is specified, iSeries Access for Web will be configured based on the default administrative server-instance already configured to run iSeries Access for Web.

- **Source web server instance:** Specify the name of the web application server administrative server/instance that has already been configured to run iSeries Access for Web.

Possible values for ASF Tomcat are:

- **Source web server instance:** Specify the name of the ASF Tomcat server that has already been configured to run iSeries Access for Web.

Share user data (SHRUSRDTA)

When configuring based on an existing iSeries Access for Web configuration, this parameter indicates if user generated data will be shared with the configuration specified in the 'Source web server type' (SRCSVRTYPE) and 'Source web server instance' (SRCSVRINST) parameters.

This value is only applicable when values are specified for the 'Source web server type' (SRCSVRTYPE) and 'Source web server instance' (SRCSVRINST) parameters.

Possible values are:

- ***NO:** The new configuration will start with a copy of the existing configuration's user generated data.
- ***YES:** The new configuration will share the user generated data with the existing configuration.

Examples for CFGACCWEB2

Configuring the WebSphere 4.0 Advanced Edition default administrative instance for port 5098:

```
CFGACCWEB2 APPSVRTYPE(*WAS40ADV) PORT(5098) WASINST(*DEFAULT).
```

Configuring an ASF Tomcat server which will share user generated data with the previous example:

```
CFGACCWEB2 APPSVRTYPE(*ASFTOMCAT) TCSRNAME(TOMCAT) TCHOMEDIR('/ASF
Tomcat/tomcat') TCUSRPRF(QTMHHTTP) SRCSVRTYPE(*WAS40ADV)
SRCSVRINST(*DEFAULT) SHRUSRDTA(*YES).
```

Configuring the WebSphere 4.0 Advanced Single Server Edition user created TESTDEPT administrative server:

```
CFGACCWEB2 APPSVRTYPE(*WAS40SNG) WASINST(TESTDEPT).
```

Error Messages for CFGACCWEB2

***ESCAPE Messages**

- IAW0001: Configure iSeries Access for Web command failed.
- IAW0009: The PORT parameter is required.
- IAW000A: The SRCSVRINST and SHRUSRDTA parameters are required.
- IAW000B: Value specified for parameter APPSVRTYPE is not valid.
- IAW000C: Value specified for parameter SRCSVRTYPE is not valid.
- IAW000D: The TCSRNAME and TCHOMEDIR and TCUSRPRF parameters are required.

STRACCWEB2 (Start iSeries Access for Web) Command

Where allowed to run: All environments (*ALL)

Threadsafe: No

The Start iSeries Access for Web (STRACCWEB2) command is used to start the iSeries Access for Web configuration within the web application server IBM WebSphere Application Server.

This command will start a configuration that was created using the Configure Access for Web (CFGACCWEB2) command.

iSeries Access for Web must be started before its functions can be accessed.

When the command runs, a Java Shell Display session starts. Status information displays, indicating what the command is processing. As the command runs, detailed status information and error information is logged to /QIBM/UserData/Access/Web2/logs/cmds.log.

iSeries Access for Web can also be started using the web application server's administration function.

Associated commands:

- CFGACCWEB2—Configure Access for Web
- ENDACCWEB2—End Access for Web
- RMVACCWEB2—Remove Access for Web

Restrictions for STRACCWEB2

1. The user of this command must have *ALLOBJ authority.
2. iSeries Access for Web must be configured using the Configure Access for Web (CFGACCWEB2) command before running this command.
3. This command is only available for the following web application servers:
 - WebSphere 4.0 Application Server Advanced Edition
4. WebSphere Advanced Edition specific restrictions
 - The WebSphere Application Server subsystem must be running and in a ready state before running this command. Refer to the WebSphere documentation for information at <http://www.ibm.com/servers/eserver/iseries/software/websphere/wsappserver> on starting the WebSphere subsystem and determining when it reaches a ready state.
5. WebSphere Advanced Single Server Edition configurations must be started using the web-based WebSphere Application Server Administrative Console.
6. ASF Tomcat configurations are automatically started when the ASF Tomcat server is started. Use the ASF Tomcat management functions available in the web-based IBM HTTP Server for iSeries function to start the ASF Tomcat server.

Parameters for STRACCWEB2

This section contains information on the required and optional parameters for STRACCWEB2.

Note: A bold, underlined value is the default value.

Table 32. STRACCWEB2 Parameters

Keyword	Description	Choices	Notes
APPSVRTYPE	Web application server type	<i>Character value</i> , *WAS40ADV	Required
WASINST	Web server instance name	<i>Character value</i> , <u>*DEFAULT</u>	Optional

Web application server type (APPSVRTYPE)

Specifies a web application server that contains a iSeries Access for Web configuration to be started.

This is a required parameter.

Possible values are:

- ***WAS40ADV**: Start iSeries Access for Web within WebSphere 4.0 Advanced Edition.

Additional values will be available as support for other web application servers is added.

Web server instance name (WASINST)

Specifies an IBM WebSphere Application Server administrative server that contains an iSeries Access for Web configuration to start.

This value is only applicable when starting for the WebSphere Application Server Advanced Edition (*WAS40ADV) web application server.

Possible values are:

- ***DEFAULT**: When IBM WebSphere Application Server was installed, a default administrative server was automatically created. When *DEFAULT is specified, iSeries Access for Web will be started within the default WebSphere administrative server.
- **Web server instance name**: Specify the name of the WebSphere administrative server that contains an iSeries Access for Web configuration to start. This is the same administrative server name that was used when the Configure Access for Web (CFGACCWEB2) command was run.

Examples for STRACCWEB2

Starting the WebSphere 4.0 Advanced Edition default administrative instance:
STRACCWEB2 APPSVRTYPE(*WAS40ADV).

Starting the WebSphere 4.0 Advanced Edition user created TESTDEPT administrative server:
STRACCWEB2 APPSVRTYPE(*WAS40ADV) WASINST(TESTDEPT).

Error Messages for STRACCWEB2

***ESCAPE Messages**

- IAW0002: Start iSeries Access for Web command failed.
- IAW000B: Value specified for parameter APPSVRTYPE is not valid.

ENDACCWEB2 (End iSeries Access for Web) Command

Where allowed to run: All environments (*ALL)

Threadsafte: No

The End iSeries Access for Web (ENDACCWEB2) command is used to end, or stop, the running iSeries Access for Web configuration within the web application server IBM WebSphere Application Server.

This command will end the running configuration that was defined using the Configure Access for Web (CFGACCWEB2) command.

When the command runs, a Java Shell Display session starts. Status information displays, indicating what the command is processing. As the command runs, detailed status information and error information is logged to /QIBM/UserData/Access/Web2/logs/cmds.log.

The iSeries Access for Web configuration can also be ended, or stopped, using the web application server's administration function.

Associated commands:

- CFGACCWEB2—Configure Access for Web
- STRACCWEB2—Start Access for Web
- RMVACCWEB2—Remove Access for Web

Restrictions for ENDACCWEB2

1. The user of this command must have *ALLOBJ authority.
2. iSeries Access for Web must be configured using the Configure Access for Web (CFGACCWEB2) command before running this command.
3. This command is only available for the following web application server types:
 - WebSphere 4.0 Application Server Advanced Edition
4. WebSphere Advanced Edition specific restrictions
 - The WebSphere Application Server subsystem must be running and in a ready state before running this command. Refer to the WebSphere documentation at <http://www.ibm.com/servers/eserver/iseries/software/websphere/wsappserver> for information on starting the WebSphere subsystem and determining when it reaches a ready state.
5. WebSphere Advanced Single Server Edition configurations must be ended using the web-based WebSphere Application Server Administrative Console.
6. ASF Tomcat configurations are automatically ended when the ASF Tomcat server is ended. Use the ASF Tomcat management functions available in the web-based IBM HTTP Server for iSeries function to end the ASF Tomcat server.

Parameters for ENDACCWEB2

This section contains information on the required and optional parameters for ENDACCWEB2.

Note: A bold, underlined value is the default value.

Table 33. ENDACCWEB2 Parameters

Keyword	Description	Choices	Notes
APPSSVRTYPE	Web application server type	<i>Character value</i> , *WAS40ADV	Required
WASINST	Web server instance name	<i>Character value</i> , <u>*DEFAULT</u>	Optional

APPSSVRTYPE

Specifies a web application server that contains a iSeries Access for Web configuration to be ended.

This is a required parameter.

Possible values are:

- ***WAS40ADV:** End the running iSeries Access for Web configuration within WebSphere 4.0 Advanced Edition. Additional values will be available as support for other web application servers is added.

Additional values will be available as support for other web application servers is added.

WASINST

Specifies an IBM WebSphere Application Server administrative server that contains an iSeries Access for Web configuration to end.

This value is only applicable when ending for the WebSphere Application Server Advanced Edition (*WAS40ADV) web application server.

Possible values are:

- ***DEFAULT:** When IBM WebSphere Application Server was installed, a default administrative server was automatically created. When *DEFAULT is specified, iSeries Access for Web will be ended within the default WebSphere administrative server.
- **Web server instance name:** Specify the name of the WebSphere administrative server that contains an iSeries Access for Web configuration to end. This is the same administrative server name that was used when the Configure Access for Web (CFGACCWEB2) command was run.

Examples for ENDACCWEB2

Ending the WebSphere 4.0 Advanced Edition default administrative server:
ENDACCWEB2 APPSVRTYPE(*WAS40ADV).

Ending the WebSphere 4.0 Advanced Edition user created TESTDEPT administrative server:
ENDACCWEB2 APPSVRTYPE(*WAS40ADV) WASINST(TESTDEPT).

Error Messages for ENDACCWEB2

***ESCAPE Messages**

- IAW0003: End iSeries Access for Web command failed.
- IAW000B: Value specified for parameter APPSVRTYPE is not valid.

RMVACCWEB2 (Remove iSeries Access for Web) Command

Where allowed to run: All environments (*ALL)

Threadsafe: No

The Remove iSeries Access for Web (RMVACCWEB2) command is used to remove the iSeries Access for Web configuration from the web application server, either IBM WebSphere Application Server or Apache Software Foundation (ASF) Tomcat.

This command will remove the configuration that was defined using the Configure Access for Web (CFGACCWEB2) command.

This command will not delete iSeries Access for Web from the server. This command will only remove the iSeries Access for Web configuration from the specified web application server.

This command will not delete user data that was generated while using iSeries Access for Web. User data was written to the following locations based on the 'Web application server type' (APPSVRTYPE) specified when the configuration was defined with the Configure Access for Web (CFGACCWEB2) command:

- *WAS40ADV - /QIBM/UserData/Access/Web2/was40adv/<instance_name>
- *WAS40SNG - /QIBM/UserData/Access/Web2/was40sng/<instance_name>

- *ASFTOMCAT - /QIBM/UserData/Access/Web2/asftomcat/<server_name>

When the command runs, a Java Shell Display session starts. Status information displays, indicating what the command is processing. As the command runs, detailed status information and error information is logged to /QIBM/UserData/Access/Web2/logs/cmds.log.

The iSeries Access for Web configuration can also be removed using the web application server's administration function. **This is not recommended!** The Remove Access for Web (RMVACCWEB2) command cleans up internal configuration information that the web application server's administration function does not.

Associated commands:

- CFGACCWEB2—Configure Access for Web
- STRACCWEB2—Start Access for Web
- ENDACCWEB2—End Access for Web

Restrictions for RMVACCWEB2

1. The user of this command must have *ALLOBJ authority.
2. iSeries Access for Web must be configured using the Configure Access for Web (CFGACCWEB2) command before running this command.
3. WebSphere Advanced Edition specific restrictions
 - When removing from WebSphere Advanced Edition, the subsystem must be running and in a ready state before running this command. Refer to the WebSphere documentation at <http://www.ibm.com/servers/eserver/iseries/software/websphere/wsappserver> for information on starting the WebSphere subsystem and determining when it reaches a ready state.
4. WebSphere Advanced Single Server Edition specific restrictions
 - After the Remove Access for Web (RMVACCWEB2) command completes, WebSphere Advanced Single Server Edition must be ended and restarted. This will remove any iSeries Access for Web configuration information that may be loaded in memory.
5. ASF Tomcat specific restrictions
 - After the Remove Access for Web (RMVACCWEB2) command completes, the ASF Tomcat server must be ended and restarted. This will remove any iSeries Access for Web configuration information that may be loaded in memory. Use the ASF Tomcat management functions available in the web-based IBM HTTP Server for iSeries function to end the ASF Tomcat server.

Parameters for RMVACCWEB2

This section contains information on the required and optional parameters for RMVACCWEB2.

Note: A bold, underlined value is the default value.

Table 34. RMVACCWEB2 Parameters

Keyword	Description	Choices	Notes
APPVRTYPE	Web application server type	<i>Character value, *WAS40ADV, *WAS40SNG, *ASFTOMCAT</i>	Required
WASINST	Web server instance name	<i>Character value, <u>*DEFAULT</u></i>	Optional

Table 34. RMVACCWEB2 Parameters (continued)

Keyword	Description	Choices	Notes
TCSRNAME	Tomcat server name	<i>Character value</i>	Optional

Web application server type (APPSVRTYPE)

Specifies a web application server that contains an iSeries Access for Web configuration to be removed.

This is a required parameter.

Possible values are:

- *WAS40ADV: Remove the iSeries Access for Web configuration within WebSphere 4.0 Advanced Edition.
- *WAS40SNG: Remove the iSeries Access for Web configuration within WebSphere 4.0 Advanced Single Server Edition.
- *ASFTOMCAT: Remove the iSeries Access for Web configuration within Apache Software Foundation Tomcat.

WASINST

Specifies an IBM WebSphere Application Server administrative server that contains an iSeries Access for Web configuration to remove.

This is only applicable when removing a configuration for the WebSphere Application Server.

Possible values are:

- ***DEFAULT**: When IBM WebSphere Application Server was installed, a default administrative server was automatically created. When *DEFAULT is specified, iSeries Access for Web will be removed from the default WebSphere administrative server.
- **Web server instance name**: Specify the name of the WebSphere administrative server that contains an iSeries Access for Web configuration to remove. This is the same administrative server name that was used when the Configure Access for Web (CFGACCWEB2) command was run.

TCSRNAME

This value specifies the name of an ASF Tomcat server that contains an iSeries Access for Web configuration to remove.

This parameter is required and applicable only when removing a configuration from the ASF Tomcat (*ASFTOMCAT) web application server.

Examples for RMVACCWEB2

Removing the WebSphere 4.0 Advanced Edition default administrative server configuration:

RMVACCWEB2 APPSVRTYPE(*WAS40ADV).

Removing the ASF Tomcat server configuration:

RMVACCWEB2 APPSVRTYPE(*ASFTOMCAT) TCSRNAME(TOMCAT).

Removing the WebSphere 4.0 Advanced Single Server Edition user created TESTDEPT administrative instance configuration:

RMVACCWEB2 APPSVRTYPE(*WAS40SNG) WASINST(TESTDEPT).

Error Messages for RMVACCWEB2

***ESCAPE Messages**

- IAW0004: Remove iSeries Access for Web command failed.
- IAW000B: Value specified for parameter APPSVRTYPE is not valid.
- IAW000E: The TCSRNAME parameter is required

Appendix F. Problems and Problem Reporting

Technical Support

See the following sources for known problems:

- iSeries Technical Support Web Site
<http://www.ibm.com/eserver/iseries/support/>
- APARs and Information APARs
http://www.ibm.com/eserver/iseries/support/n_dir/nas4apar.nsf/nas4aparhome
- Support Line Knowledge Base
<http://www.ibm.com/eserver/iseries/support/supporthome.nsf/Document/10000051>
- iSeries Access Information APARs (known problems and support statements)
<http://www.ibm.com/eserver/iseries/access/caiiapar.htm>
- iSeries Access Frequently Asked Questions (marketing, strategy, ordering, support, links to forums, etc.)
<http://www.ibm.com/eserver/iseries/access/cafaq.htm>
- Host Publisher Support/Server Packs
<http://www.ibm.com/software/webservers/hostpublisher>

For other sources of information for iSeries Access for Web, see Appendix A, "Sources of Information for iSeries Access for Web" on page 109.

Problem Reporting—Gathering Information for IBM Support

If you decide to open a problem record to IBM Support, have the following information available when you place the call:

- **The level of iSeries Access for Web-** The level of iSeries Access for Web is displayed as part of the footer on any of the iSeries Access for Web or About panels.
- The iSeries Cumulative PTF level - Type DSPPTF (Display Program Temporary Fix) on the iSeries command prompt. Record the first PTF ID in the list. It will have the format Tzxxyyy where xx is the year, yyy is the julian date and z is either L or C.
- The IBM Operating System/400 (OS/400) version (for example, V5R1M0) - You can also find this at the DSPPTF screen. Record the Release field at the top of the screen.
- A description of what you were attempting when the failure occurred.
- The exact text and error numbers of any error message that the web browser displayed.
- Any VLOGs that are generated at the time the error occurred, if the VLOGs have any of the following codes:
 - Major code of 0700 and a minor code of either F230 or F299
 - Major code of 4400 and any minor code
 - Major code of 4401 and any minor code

Appendix G. Notices

This information was developed for products and services offered in the U.S.A. IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe upon any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
500 Columbus Avenue
Thornwood, NY 10594
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

Licensees of this program who want to have information about it for the purpose of enabling: (i) the exchange of information between independently created

programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
Software Interoperability Coordinator
3605 Highway 52 N
Rochester, MN 55901-7829
U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this information and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement, or any equivalent agreement between us.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. You may copy, modify, and distribute these sample programs in any form without payment to IBM for the purposes of developing, using, marketing, or distributing application programs conforming to IBM's application programming interfaces.

Code disclaimer information

This document contains programming examples.

IBM grants you a nonexclusive copyright license to use all programming code examples from which you can generate similar function tailored to your own specific needs.

All sample code is provided by IBM for illustrative purposes only. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs.

All programs contained herein are provided to you "AS IS" without any warranties of any kind. The implied warranties of non-infringement, merchantability and fitness for a particular purpose are expressly disclaimed.

Trademarks

The following terms are trademarks of International Business Machines Corporation in the United States, or other countries, or both:

AFP
Application System/400
AS/400
Client Access
e (logo)
IBM
iSeries
iSeries
Operating System/400
OS/400
Redbooks
WebSphere
400

Lotus and 1-2-3 are registered trademarks of Lotus Development Corporation in the United States, other countries, or both.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Microsoft, Windows, and Windows NT are trademarks of Microsoft Corporation in the United States, other countries, or both.

Pentium® is a trademark or registered trademark of Intel Corporation in the United States, other countries, or both.

Other company, product, and service names may be trademarks or service marks of others.

Index

A

administrative instances
 WebSphere 19
AFP
 restrictions 69
AFP viewer 43
authentication 33

C

CFGACCWEB2 117
 error messages 121
 examples 121
 parameters 118
 restrictions 118
character set 113
character sets policies 78
CL commands 117
Coded Character Set ID (CCSID) 114
Command 62
 policies 91
 previously run 64
 saved 64
 search 62
command prompt 62
 restrictions 72
configure
 iSeries Access for Web 117
connection pool 66
cookies
 Microsoft Internet Explorer 15
 Netscape 14
 Opera 15
copy data to table 54
 XML considerations 55
Customize 65
 deny access to functions 103
 group profiles 66
 home page 105
 policies 94
 preferences 65
 selected profile 66
 user profiles 65
 users and groups 101

D

Database 49
 JDBC 58
 new relational table 57
 policies 85
 restrictions 69
 saved requests 51
 shortcut 51
 tables 50
digital certificates 34
 configure 35
Document Library Services (QDLS) file
 system 115

E

ENDACCWEB2 123
 error messages 125
 examples 125
 parameters 124
 restrictions 124
ending iSeries Access for Web 123
error messages
 CFGACCWEB2 121
 ENDACCWEB2 125
 RMVACCWEB2 128
 STRACCWEB2 123
exit programs 33

F

File Action column 59
file shares 60
Files 58
 content-type (MIME-type)
 mapping 60
 policies 88
 restrictions 72

G

groups
 *PUBLIC profile 103
 customize 101

H

home page
 customize 105
Host Publisher 27
 PTFs 17
Host Publisher Studio 27
HTML output
 creating 53
HTTP server
 port 18
HTTP server powered by Apache
 configure for SSL 35
 creation 19
 setup 23
HTTPS 34

I

Infoprint Server 42
Information APAR 109
iSeries Access for Web
 beta release 15
 configure 25, 117
 delete 31
 end 123
 install 16
 license information 13
 PTFs 17

iSeries Access for Web (*continued*)

 remove 125
 start 121
 verify the installation 29

J

Jobs 61
 policies 82

L

language policies 77
languages 113
license information 5, 13

M

Mail 64
 policies 92
message queues 49
Messages 46
 display 47
 policies 81
 restrictions 69
 send 48
Microsoft Internet Explorer 15
My Folder 65
 policies 93

N

Netscape 14
NLS Considerations 113

O

object level security 33
Opera 15
 restrictions 72
original HTTP server
 configure for SSL 34
 creation 21
Other
 policies 96
output queues 46

P

page layout policies 75
password
 change 66
PDF
 font settings 53
 printer output 43
 Run SQL 53
performance tuning 30

policies
 character sets 78
 Command 91
 Customize 94
 Database 85
 Files 88
 Jobs 82
 language 77
 Mail 92
 Messages 81
 My Folder 93
 Other 96
 page layout 75
 Print 78

port
 HTTP server 18
 SSL 36

Preferences 99
 restrict access 100
 use 99

Print
 policies 78
 restrictions 69

printer output 42
 PDF 43

printer shares 46

Printers 44

Problems and Problem Reporting 129

PTFs 16, 109
 Host Publisher 17
 installing 16
 iSeries Access for Web 17
 Tomcat 17
 WebSphere 17

Q

QDLS 115

R

removing iSeries Access for Web 125
restrictions

 AFP 69
 CFGACCWEB2 118
 command prompt 72
 Database 69
 ENDACCWEB2 124
 Files 72
 Messages 69
 Opera 72
 Print 69
 RMVACCWEB2 126
 Run SQL 70
 STRACCWEB2 122
 RMVACCWEB2 125
 error messages 128
 examples 127
 parameters 126
 restrictions 126

Run SQL 51
 HTML output 53
 PDF output 53
 restrictions 70
 XML output 52

S

Save and Restore 111
secure sockets layer (SSL) 34
spooled files 42
SSL 34
 encryption software requirements 14
 port 36
start
 iSeries Access for Web 121
STRACCWEB2 121
 error messages 123
 examples 123
 parameters 122
 restrictions 122

T

Tomcat
 PTFs 17
 setup 24
 software requirements 13

U

users
 customize 101
 policy settings 101

W

WebSphere
 administrative instances 19
 HTTP server creation 19
 PTFs 17
 software requirements 12
WebSphere Advanced Edition
 verify setup 22
WebSphere Advanced Single Server
 Edition
 verify setup 22

X

XML
 copy data to table 55
XML output
 creating 52

Readers' Comments — We'd Like to Hear from You

iSeries
iSeries Access for Web
Version 5

Publication No. SC41-5518-01

Overall, how satisfied are you with the information in this book?

	Very Satisfied	Satisfied	Neutral	Dissatisfied	Very Dissatisfied
Overall satisfaction	<input type="checkbox"/>				

How satisfied are you that the information in this book is:

	Very Satisfied	Satisfied	Neutral	Dissatisfied	Very Dissatisfied
Accurate	<input type="checkbox"/>				
Complete	<input type="checkbox"/>				
Easy to find	<input type="checkbox"/>				
Easy to understand	<input type="checkbox"/>				
Well organized	<input type="checkbox"/>				
Applicable to your tasks	<input type="checkbox"/>				

Please tell us how we can improve this book:

Thank you for your responses. May we contact you? Yes No

When you send comments to IBM, you grant IBM a nonexclusive right to use or distribute your comments in any way it believes appropriate without incurring any obligation to you.

Name

Address

Company or Organization

Phone No.

Readers' Comments — We'd Like to Hear from You
SC41-5518-01



Cut or Fold
Along Line

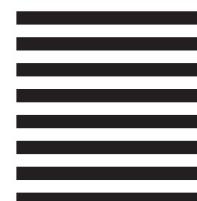
Fold and Tape

Please do not staple

Fold and Tape



NO POSTAGE
NECESSARY
IF MAILED IN THE
UNITED STATES



BUSINESS REPLY MAIL

FIRST-CLASS MAIL PERMIT NO. 40 ARMONK, NEW YORK

POSTAGE WILL BE PAID BY ADDRESSEE

IBM CORPORATION
ATTN DEPT 542 IDCLERK
3605 HWY 52 N
ROCHESTER MN 55901-7829



Fold and Tape

Please do not staple

Fold and Tape

SC41-5518-01

Cut or Fold
Along Line

IBM[®]

Printed in U.S.A.

SC41-5518-01

